

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-031204

(43)Date of publication of application : 02.02.1999

(51)Int.Cl.

G06K 17/00

G06F 17/60

G07B 5/00

G07F 7/12

G09C 1/00

H04L 9/32



(21)Application number : 09-188064

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 14.07.1997

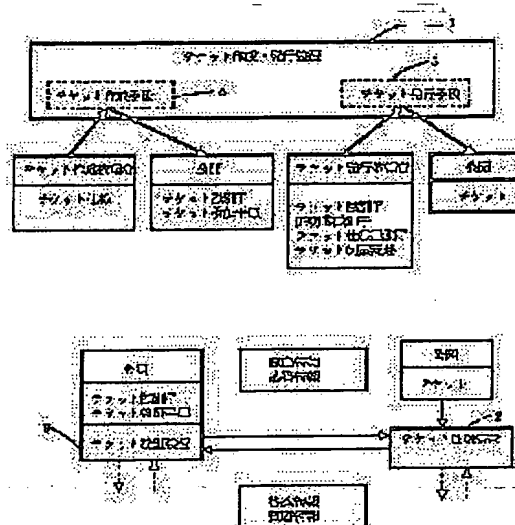
(72)Inventor : TERAO TARO  
KAMEI MITSUHIKA  
NAKATSUYAMA HISASHI

## (54) ELECTRONIC TICKET SYSTEM

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To make illegal use by forgery or duplication extremely difficult, to certify the content of a ticket to a third person, and to maintain the anonymity of a user at the time of using the ticket in an electronic ticket using environment.

**SOLUTION:** A ticket preparing part 4 of a ticket preparing and issuing device 1 prepares the specification of a ticket corresponding to a prescribed service or article based on a ticket preparation request. A ticket issuing part 5 issues a corresponding ticket by inputting a ticket identifier, certifier identifier, ticket specification identifier, and ticket additional information based on a ticket issue request. A ticket certifying device 2 holds the ticket issued by the ticket issuing part 5, and certifies the holding of the ticket by communicating with a ticket verifying device 3. The ticket verifying device 3 holds the ticket identifier and a ticket verification procedure prepared by the ticket preparing means 4, and operates the verification of the ticket by communicating with the ticket certifying device 2.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's  
decision of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 1 1 - 3 1 2 0 4

(43) 公開日 平成 1 1 年 (1 9 9 9) 2 月 2 日

(51) Int. Cl. °	識別記号	庁内整理番号	F I	技術表示箇所
G06K 17/00			G06K 17/00	T
G06F 17/60			G07B 5/00	Z
G07B 5/00			G09C 1/00	640 C
G07F 7/12			G06F 15/21	340 C
G09C 1/00	640		G07F 7/08	C

審査請求 未請求 請求項の数 6 1 O L (全 4 9 頁) 最終頁に続く

(21) 出願番号 特願平 9 - 1 8 8 0 6 4

(22) 出願日 平成 9 年 (1 9 9 7) 7 月 1 4 日

(71) 出願人 0 0 0 0 0 5 4 9 6  
富士ゼロックス株式会社  
東京都港区赤坂二丁目 1 7 番 2 2 号

(72) 発明者 寺尾 太郎  
神奈川県足柄上郡中井町境 4 3 0 グリー  
ンテクなかい 富士ゼロックス株式会社内

(72) 発明者 亀井 光久  
神奈川県足柄上郡中井町境 4 3 0 グリー  
ンテクなかい 富士ゼロックス株式会社内

(72) 発明者 中津山 恒  
神奈川県足柄上郡中井町境 4 3 0 グリー  
ンテクなかい 富士ゼロックス株式会社内

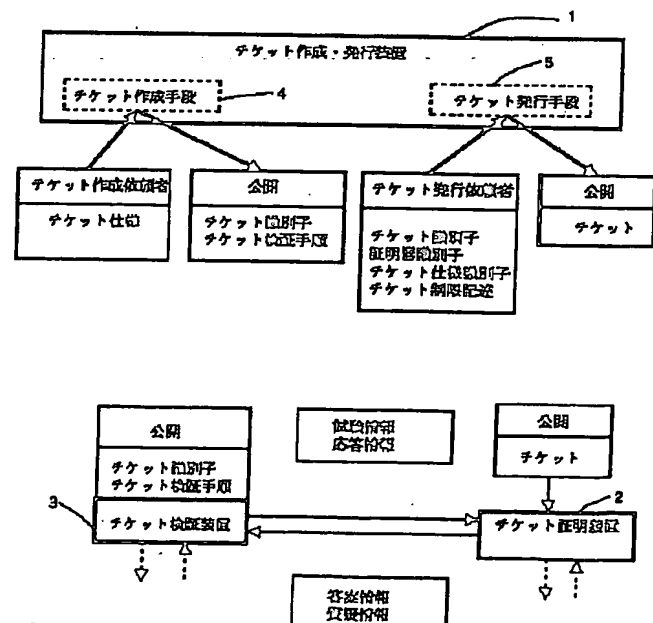
(74) 代理人 弁理士 澤田 俊夫

(54) 【発明の名称】 電子チケットシステム

## (57) 【要約】

【課題】 電子チケット利用環境において、偽造や複製などによる不正利用が非常に難しく、チケットの内容を第三者に証明でき、かつ、チケットの利用時に利用者の匿名性が維持されるようにする。

【解決手段】 チケット作成・発行装置 1 のチケット作成部 4 は、チケット作成依頼に基づいて、所定のサービスや物に対応するチケットの仕様を作成する。チケット発行部 5 は、チケット発行依頼に基づいて、チケット識別子と証明器識別子とチケット仕様識別子とチケット付加情報を入力として、対応するチケットを発行する。チケット検証装置 2 は、チケット発行部 5 の発行したチケットを保持し、チケット検証装置 3 と通信を行ないチケットの保有を証明する。チケット検証装置 3 は、チケット作成手段 4 の作成したチケット識別子とチケット検証手順を保持し、チケット証明装置 2 と通信を行ないチケットの検証を行なう。



## 【特許請求の範囲】

【請求項 1】 チケット発行装置、チケット認証装置からなる電子チケットシステムであって、上記チケット発行装置は、少なくともチケット公開情報およびチケット秘密情報を保持するチケット特徴情報保持手段と、チケット利用者固有情報を保持するチケット利用者固有情報保持手段と、少なくとも上記チケット秘密情報および上記チケット利用者固有情報から、チケットを作成するチケット発行手段とからなり、上記チケット認証装置は、チケット利用者固有情報保持手段と、チケット保持手段と、少なくともチケット利用者固有情報とチケットから前記チケットの正しさを検証する検証手段とからなることを特徴とする電子チケットシステム。

【請求項 2】 チケット発行装置、検証装置、証明装置からなる電子チケットシステムであって、上記チケット発行装置は、少なくともチケット公開情報とチケット秘密情報を保持するチケット特徴情報保持手段と、証明装置固有情報保持手段と、少なくともチケット秘密情報と証明装置固有情報から、デジタル情報であるチケットを作成するチケット発行手段とからなり、上記検証装置は、対話証明で用いられる値を生成する認証情報生成手段と、上記証明装置がチケット秘密情報を算出できたか否かを検証する対話検証手段とからなり、上記証明装置は、証明装置固有情報保持手段と、チケット保持手段と、少なくとも証明装置固有情報とチケットとからチケット秘密情報に関する知識の証明を行なえる対話証明手段とからなることを特徴とする電子チケットシステム。

【請求項 3】 請求項 2 の電子チケットシステムであって、上記チケット発行装置は、チケット特徴情報を作成できるチケット特徴情報作成手段を備えたことを特徴とする電子チケットシステム。

【請求項 4】 請求項 2 または 3 記載の電子チケットシステムであって、上記チケット発行装置は、証明装置識別情報を証明装置固有情報と関連づけて保持する証明装置識別情報保持手段を備えたことを特徴とする電子チケットシステム。

【請求項 5】 請求項 2、3 または 4 記載の電子チケットシステムであって、チケット特徴情報は少なくともチケット公開情報とチケット秘密情報からなることを特徴とする電子チケットシステム。

【請求項 6】 請求項 5 記載の電子チケットシステムであって、チケット公開情報が有限アーベル群であり、チケット秘密情報がその零化域であることを特徴とする電子チケットシステム。

【請求項 7】 請求項 5 記載の電子チケットシステムであって、チケット秘密情報が整数であり、チケット公開情報が有限群とその元とその元の位数とその元の秘密情報倍であることを特徴とする電子チケットシステム。

【請求項 8】 請求項 2 ～ 7 のいずれかに記載の電子チケットシステムであって、証明装置は可変な内部状態を

保持する内部状態保持手段を備えたことを特徴とする電子チケットシステム。

【請求項 9】 請求項 8 記載の電子チケットシステムであって、上記証明装置の内部状態保持手段が保持する可変な内部状態の少なくとも一部は外部から書き換え不能であることを特徴とする電子チケットシステム。

【請求項 10】 請求項 9 記載の電子チケットシステムであって、上記証明装置は初期化が行なわれた内部状態を示す情報を保持するチケットカウント手段を備えたことを特徴とする電子チケットシステム。

【請求項 11】 請求項 8、9、または 10 記載の電子チケットシステムであって、対話検証および対話証明の過程で少なくとも 1 度の秘密情報に関する知識の証明の観点から冗長な情報伝達を行なうことを特徴とする電子チケットシステム。

【請求項 12】 請求項 10 記載の電子チケットシステムであって、少なくとも 1 度は証明装置の内部情報から得られる情報を上記証明装置から上記検証装置に伝達することを特徴とする電子チケットシステム。

【請求項 13】 請求項 12 記載の電子チケットシステムであって、少なくとも 1 度は、外部から書き換え不能な上記証明装置の内部情報から得られる情報を上記証明装置から上記検証装置に伝達することを特徴とする電子チケットシステム。

【請求項 14】 請求項 9 または 10 記載の電子チケットシステムであって、上記証明装置の内部状態保持手段はチケットの有効性を示す内部状態をチケットと関連づけて外部から書き換え不能な形で保持し、上記チケットの有効性を示す内部状態が特定の値であるときには、対応するチケットが無効であるものとして、対話証明時に伝達する情報として正しくないものを伝達することを特徴とする電子チケットシステム。

【請求項 15】 請求項 14 記載の電子チケットシステムであって、上記検証装置は少なくとも 1 度、上記証明装置に情報を伝達し、上記証明装置は、上記検証装置から伝達される情報にしたがって、チケットと関連付けられた、チケットの有効性を示す内部状態を変更して、有効なチケットの無効化あるいは無効となったチケットの有効化を行なうことを特徴とする電子チケットシステム。

【請求項 16】 請求項 9 または 10 記載の電子チケットシステムであって、上記証明装置の内部状態保持手段は、チケットのカウンタとして機能する内部状態をチケットと関連づけ、外部から書き換え不能な形で保持し、対話証明の過程でチケットのカウンタとして機能する内部状態を用いて演算を行ない、演算結果が所定の値であるときには、対応するチケットが無効であるものとして、対話証明時に伝達する情報として正しくないものを伝達することを特徴とする電子チケットシステム。

【請求項 17】 請求項 16 の電子チケットシステムで

あって、上記検証装置は少なくとも1度、上記証明装置に情報を伝達し、上記証明装置は、上記検証装置から伝達される情報にしたがって、チケットと関連付けられた、チケットのカウンタとして機能する内部状態を設定することを特徴とする電子チケットシステム。

【請求項 1 8】 請求項 2 ～ 1 7 のいずれかに記載の電子チケットシステムであって、上記証明装置は複数の対話検証手続きを実行可能な証明手順実行部を備え、チケット特徴情報の一部を用いて、適切な証明手順を選択し、対話証明を実行することを特徴とする電子チケットシステム。

【請求項 1 9】 請求項 2 ～ 1 7 のいずれかに記載の電子チケットシステムであって、上記証明装置は対話検証手続きの少なくとも一部のステップを記述したプログラムを実行可能な証明手順実行部を備え、チケット特徴情報の一部からプログラムを抽出し、対話証明を実行することを特徴とする電子チケットシステム。

【請求項 2 0】 請求項 2 ～ 1 9 のいずれかに記載の電子チケットシステムであって、上記検証装置は、対話検証手続きにおいて、上記検証装置および上記証明装置間で通信された情報、あるいはその一部、あるいはそれらに所定の演算を施して生成した情報を保存することを特徴とする電子チケットシステム。

【請求項 2 1】 請求項 2 ～ 2 0 のいずれかに記載の電子チケットシステムであって、上記検証装置は対話検証手続きにおいて上記証明装置に伝達した情報の生成に利用した情報と、上記証明装置が上記情報に演算を施して応答した情報の組を保存することを特徴とする電子チケットシステム。

【請求項 2 2】 請求項 2 ～ 2 1 のいずれかに記載の電子チケットシステムであって、上記検証装置は、上記検証装置の固有情報を保持する検証装置固有情報保持手段と、チケットを保持するチケット保持手段を備え、対話検証においてチケットからの情報を利用することを特徴とする電子チケットシステム。

【請求項 2 3】 請求項 2 ～ 2 2 のいずれかに記載の電子チケットシステムであって、上記証明装置は、認証情報とチケット公開情報とチケットとチケット付加情報と証明装置固有情報とより所定の方法で証明情報を計算することを特徴とする電子チケットシステム。

【請求項 2 4】 請求項 2 3 の電子チケットシステムであって、チケットの秘密情報が  $D$  であり、チケットの公開情報が  $(n, E)$  であり、 $\lambda(n)$  が法  $n$  の下で位数が最大となる数の位数であり、 $ED \equiv 1 \pmod{\lambda(n)}$  であり、チケットの付加情報が  $L$  であり、証明装置固有情報が秘密の一方方向性関数  $d_s(L, n)$  であり、チケットが  $t := D - d_s(L, n)$  で与えられているとき、上記証明装置は、認証情報  $C$  に対して、証明情報  $R$  を  $C$  の法  $n$  での  $t$  による冪乗と、 $C$  の法  $n$  での一方方向性関数値  $d_s(L, n)$  を指数とする冪乗との法  $n$

での積  $C^t C^{d_s(L, n)} \pmod{n}$  として証明情報を計算することを特徴とする電子チケットシステム。

【請求項 2 5】 請求項 2 3 記載の電子チケットシステムであって、チケットの秘密情報が  $D$  であり、チケットの公開情報が  $(n, E)$  であり、 $ED \equiv 1 \pmod{\lambda(n)}$  であり、チケットの付加情報が  $L$  であり、証明装置固有情報が秘密の値  $d_s$  であり、 $f(d_s, L, n)$  を一方方向性関数として、チケットが  $t := D - f(d_s, L, n)$  で与えられているとき、上記証明装置は、認証情報  $C$  に対して、証明情報  $R$  を  $C$  の法  $n$  での  $t$  による冪乗と、 $C$  の法  $n$  での一方方向性関数値  $f(d_s, L, n)$  を指数とする冪乗との法  $n$  での積  $C^t C^{f(d_s, L, n)} \pmod{n}$  として証明情報を計算することを特徴とする電子チケットシステム。

【請求項 2 6】 請求項 2 3 記載の電子チケットシステムであって、チケットの秘密情報が  $x$  であり、 $p$  が素数であり、 $G$  が離散対数問題が困難な有限群であり、 $g$  が有限群  $G$  の位数  $p$  の元であり、チケットの公開情報が  $(p, G, g, y)$  であり、 $y = g^x$  であり、チケットの付加情報が  $L$  であり、証明装置固有情報が秘密の一方方向性関数  $d_s(L, y)$  であり、チケットが  $t := x - d_s(L, y)$  で与えられているとき、上記証明装置は、認証情報  $C$  に対して、証明情報  $R$  を  $C$  の  $t$  を指数とする冪乗と、 $C$  の一方方向性関数値  $d_s(L, y)$  を指数とする冪乗との積  $C^t C^{d_s(L, y)}$  として証明情報を計算することを特徴とする電子チケットシステム。

【請求項 2 7】 請求項 2 3 記載の電子チケットシステムであって、チケットの秘密情報が  $x$  であり、チケットの公開情報が  $(p, G, g, y)$  であり、 $y = g^x$  であり、チケットの付加情報が  $L$  であり、証明装置固有情報が秘密の値  $d_s$  であり、 $f(d_s, L, y)$  を一方方向性関数として、チケットが  $t := x - f(d_s, L, y)$  で与えられているとき、上記証明装置は、認証情報  $C$  に対して、証明情報  $R$  を  $C$  の  $t$  を指数とする冪乗と、 $C$  の一方方向性関数値  $f(d_s, L, y)$  を指数とする冪乗との積  $C^t C^{f(d_s, L, y)}$  として証明情報を計算することを特徴とする電子チケットシステム。

【請求項 2 8】 請求項 2 3 記載の電子チケットシステムであって、上記検証装置は、認証情報と証明情報とチケット公開情報とより証明情報が正しいかどうかを判定し、証明情報が正しい場合は、証明情報に埋め込まれた情報を導出することを特徴とする電子チケットシステム。

【請求項 2 9】 請求項 2 8 記載の電子チケットシステムであって、上記検証装置は、認証情報  $C$  と証明情報  $R$  とチケット公開情報  $(n, E)$  との場合、証明情報  $R$  を法  $n$  で  $E$  乗したものを  $C$  と比較し、あるビット列  $M$  があって  $R^E \pmod{n} = C \parallel M$  ( $C$  と  $M$  とのビット連結) となっていれば証明情報は正しいと判定し、証明情報が正しい場合は  $M$  を証明情報に埋め込まれた情報とし

て導出することを特徴とする電子チケットシステム。

【請求項30】 請求項28記載の電子チケットシステムであって、上記検証装置は、認証情報Cと証明情報Rとチケット公開情報(n, E)との場合、Iを予め与えた限界として、ある $M < I$ に対して、証明情報Rを法nで $E^I$ 乗したものとCとが等しければ証明情報は正しいと判定し、証明情報が正しい場合はMを証明情報に埋め込まれた情報として導出することを特徴とする電子チケットシステム。

【請求項31】 請求項23記載の電子チケットシステムであって、上記証明装置は、チケットとチケット付加情報と証明装置固有情報とより所定の方法でチケット秘密情報を計算し、認証情報に対して、前記チケット秘密情報を用いた計算を施すことによって証明情報を生成することを特徴とする電子チケットシステム。

【請求項32】 請求項31記載の電子チケットシステムであって、チケットの秘密情報がDであり、チケットの付加情報がLであり、証明装置固有情報がある暗号系の復号鍵 $d_0$ であり、証明装置固有情報に対応する暗号化を $E_0$ として、上記証明装置は、チケットが $t := E_0(D || L)$ で与えられているとき、チケットtを $d_0$ によって復号してチケット秘密情報Dとチケット付加情報Lを計算することを特徴とする電子チケットシステム。

【請求項33】 請求項31記載の電子チケットシステムであって、チケットの秘密情報がDであり、チケットの付加情報がLであり、証明装置固有情報がある暗号系の復号鍵 $d_0$ であり、証明装置固有情報に対応する暗号化を $E_0$ とし、 $h(L)$ を一方方向性関数として、上記証明装置は、チケットが $t := E_0(D || h(L))$ で与えられているとき、チケットtを $d_0$ によって復号してチケット秘密情報Dを計算し、チケット付加情報Lの一方方向性関数値 $h(L)$ を計算することにより、Lの完全性を検証することを特徴とする電子チケットシステム。

【請求項34】 請求項31記載の電子チケットシステムであって、チケットの秘密情報がDであり、チケットの付加情報がLであり、証明装置固有情報がある暗号系の復号鍵 $d_0$ であり、証明装置固有情報に対応する暗号化を $E_0$ とし、 $h(L)$ を一方方向性関数として、チケットが $t := (E_0(D), h(d_0 || D || L))$ で与えられているとき、上記証明装置はチケットtの第1成分を $d_0$ によって復号してチケット秘密情報Dを計算し、チケットtの第2成分と一方方向性関数値 $h(d_0 || D || L)$ とを比較することによってチケット付加情報Lの完全性を検証することを特徴とする電子チケットシステム。

【請求項35】 請求項28～30のいずれかに記載の電子チケットシステムであって、上記証明装置は、出力情報保持手段を持ち、前記チケット秘密情報を用いた計

算を施す際に、出力情報保持手段に保持された出力情報と認証情報より証明情報を計算することを特徴とする電子チケットシステム。

【請求項36】 請求項35記載の電子チケットシステムであって、上記証明装置は、出力情報保持手段を持ち、チケットの秘密情報をDとし、出力情報保持手段に保持された出力情報をMとし、認証情報をCとすると、証明情報を

【数1】

$$C D^M \bmod n$$

として計算することを特徴とする電子チケットシステム。

【請求項37】 請求項35記載の電子チケットシステムであって、上記証明装置は、出力情報保持手段を持ち、前記チケット秘密情報を用いた計算を施す前に、出力情報保持手段に保持された出力情報を用いて認証情報を更新することを特徴とする電子チケットシステム。

【請求項38】 請求項37記載の電子チケットシステムであって、上記証明装置は、出力情報保持手段を持ち、出力情報保持手段に保持された出力情報をMとし、認証情報をCとすると、認証情報を $C || M$ に更新することを特徴とする電子チケットシステム。

【請求項39】 請求項23記載の電子チケットシステムであって、上記証明装置は、第2の認証情報生成手段を持ち、第2の認証情報と第2の証明情報とチケット付加情報とより第2の証明情報が正しいかどうかを判定し、第2の証明情報が正しい場合、上記証明装置の内部状態を更新することを特徴とする電子チケットシステム。

【請求項40】 請求項39記載の電子チケットシステムであって、チケット付加情報Lは少なくとも上記検証装置を検証するための情報 $v || \epsilon$ の一部を含み、 $\epsilon$ と $\lambda(v)$ は互いに素として、上記証明装置は、第2の認証情報 $x$ と第2の証明情報 $\rho$ が

【数2】

$$x = \rho^* \bmod v$$

を満たすときに第2の証明情報が正しいと判定することを特徴とする電子チケットシステム。

【請求項41】 請求項39記載の電子チケットシステムであって、チケット付加情報Lは少なくとも $\eta$ の一部を含み、上記証明装置は、第2の認証情報 $g'$ と第2の証明情報 $\rho$ が

【数3】

$$\rho = \eta^* \bmod p$$

を満たすときに第2の証明情報が正しいと判定することを特徴とする電子チケットシステム。

【請求項42】 請求項39記載の電子チケットシステムであって、上記証明装置は、入力情報保持手段を持ち、第2の証明情報が正しい場合は、第2の証明情報に

埋め込まれた入力情報を導出し、入力情報保持手段に保持することを特徴とする電子チケットシステム。

【請求項 4 3】 請求項 4 2 記載の電子チケットシステムであって、チケット付加情報 L は少なくとも  $\nu \parallel \varepsilon$  の一部を含み、 $\varepsilon$  と  $\lambda$  ( $\nu$ ) は互いに素として、上記証明装置は、第 2 の認証情報  $x$  と第 2 の証明情報  $\rho$  があるビット列  $\mu$  に対して、

【数 4】

$$x \parallel \mu = \rho^e \bmod \nu$$

を満たすときに第 2 の証明情報が正しいと判定し、 $\mu$  を第 2 の証明情報に埋め込まれた入力情報として入力情報保持手段に保持することを特徴とする電子チケットシステム。

【請求項 4 4】 請求項 4 2 記載の電子チケットシステムであって、チケット付加情報 L は少なくとも  $\nu \parallel \varepsilon$  の一部を含み、上記証明装置は、第 2 の認証情報  $x$  と第 2 の証明情報  $\rho$  が 1 を予め与えた限界として、ある  $\mu < 1$  に対して、

【数 5】

$$x = \rho^{\varepsilon \mu} \bmod \nu$$

を満たすときに第 2 の証明情報が正しいと判定し、 $\mu$  を第 2 の証明情報に埋め込まれた入力情報として入力情報保持手段に保持することを特徴とする電子チケットシステム。

【請求項 4 5】 請求項 2 3 記載の電子チケットシステムであって、上記証明装置は、入力情報保持手段を持ち、入力情報保持手段に保持された入力情報に基づいて内部状態保持手段に保持された内部状態を更新することを特徴とする電子チケットシステム。

【請求項 4 6】 請求項 2 3 記載の電子チケットシステムであって、上記証明装置は、認証情報とチケット付加情報とに基づいて、証明情報を正しく生成するか否かを判定することを特徴とする電子チケットシステム。

【請求項 4 7】 請求項 2 3 記載の電子チケットシステムであって、上記証明装置は、内部状態とチケット付加情報とに基づいて、証明情報を正しく生成するか否かを判定することを特徴とする電子チケットシステム。

【請求項 4 8】 請求項 2 3 記載の電子チケットシステムであって、上記証明装置は、内部状態とチケット付加情報とに基づいて、出力情報を計算し、出力情報保持手段に保持することを特徴とする電子チケットシステム。

【請求項 4 9】 請求項 2 3 記載の電子チケットシステムであって、上記検証装置は、第 2 の認証情報と特権を表す秘密情報とより第 2 の証明情報を生成することを特徴とする電子チケットシステム。

【請求項 5 0】 請求項 4 9 記載の電子チケットシステムであって、特権を表す秘密情報を  $\delta$  として、対応する公開情報を ( $\nu$ ,  $\varepsilon$ ) として、 $\varepsilon \delta \equiv 1 \bmod \lambda$  ( $\nu$ ) が満たされるとき、上記検証装置は、第 2 の認証

情報  $x$  より第 2 の証明情報  $\rho$  を

【数 6】

$$\rho := x^e \bmod \nu$$

として生成することを特徴とする電子チケットシステム。

【請求項 5 1】 請求項 4 9 記載の電子チケットシステムであって、特権を表す秘密情報を  $\eta$  として、対応する公開情報を ( $p$ ,  $g$ ,  $q$ ,  $\eta$ ) として、

【数 7】

$$\eta = g^f \bmod p$$

が満たされるとき、上記検証装置は、第 2 の認証情報  $x$  より第 2 の証明情報  $\rho$  を

【数 8】

$$\rho := x^f \bmod p$$

として生成することを特徴とする電子チケットシステム。

【請求項 5 2】 請求項 4 9、5 0 または 5 1 記載の電子チケットシステムであって、上記検証装置は、入力情報保持手段を持ち、前記特権を表す秘密情報を用いた計算を施す際に、入力情報保持手段に保持された入力情報と第 2 の認証情報をより第 2 の証明情報を計算することを特徴とする電子チケットシステム。

【請求項 5 3】 請求項 5 2 記載の電子チケットシステムであって、特権を表す秘密情報を  $\delta$  として、対応する公開情報を ( $\nu$ ,  $\varepsilon$ ) として、 $\varepsilon \delta \equiv 1 \bmod \lambda$  ( $\nu$ ) が満たされるとき、上記検証装置は、入力情報保持手段に保持された入力情報  $\mu$  と第 2 の認証情報  $x$  より第 2 の証明情報  $\rho$  を

【数 9】

$$\rho := x^{\delta \mu} \bmod \nu$$

として生成することを特徴とする電子チケットシステム。

【請求項 5 4】 請求項 4 9、5 0 または 5 1 記載の電子チケットシステムであって、上記検証装置は、入力情報保持手段を持ち、前記特権を表す秘密情報を用いた計算を施す前に、入力情報保持手段に保持された入力情報を用いて第 2 の認証情報を更新することを特徴とする電子チケットシステム。

【請求項 5 5】 請求項 5 4 記載の電子チケットシステムであって、上記検証装置は、入力情報保持手段を持ち、入力情報保持手段に保持された入力情報を  $\mu$  とし、第 2 の認証情報を  $x$  とすると、第 2 の認証情報を  $x \parallel \mu$  に更新することを特徴とする電子チケットシステム。

【請求項 5 6】 権利を表徴するデジタル情報からなるチケットを発行する電子チケット発行装置において、少なくともチケット秘密情報を保持するチケット特徴情報保持手段と、チケット利用者固有情報を保持するチケット利用者固有情報保持手段と、

少なくとも上記チケット秘密情報および上記チケット利用者固有情報から、チケットを作成するチケット発行手段とからなることを特徴とする電子チケット発行装置。

【請求項 5 7】 権利を表象するデジタル情報からなる電子チケットにおいて、少なくともチケット秘密情報およびチケット利用者固有情報に所定の演算を実行して生成されたことを特徴とする電子チケット。

【請求項 5 8】 権利を表象するデジタル情報からなる電子チケットを記録する記録装置において、上記電子チケットが、少なくともチケット秘密情報およびチケット利用者固有情報に所定の演算を実行して生成されたことを特徴とする電子チケット用記録装置。

【請求項 5 9】 権利を表象するデジタル情報からなるチケットを用いて上記権利を有することを証明する電子チケット証明装置において、

チケット利用者固有情報を保持するチケット利用者固有情報保持手段と、

少なくともチケット秘密情報と上記チケット利用者固有情報とから生成されたデジタル情報からなるチケットを保持するチケット保持手段と、

少なくとも上記チケット利用者固有情報と上記チケットから上記チケット秘密情報なしには生成できない証明情報を生成する証明手段とを有することを特徴とする証明装置。

【請求項 6 0】 権利を表象するデジタル情報からなるチケットを用いて電子チケット証明装置により生成された証明情報を検証して上記電子チケット証明装置の担持者が上記権利を有することを検証する電子チケット検証装置において、

認証用の情報を生成する手段と、

少なくともチケット秘密情報とチケット証明装置の固有情報とから生成されたデジタル情報からなるチケットと、上記チケット証明装置の固有情報とに基づいて生成された証明情報が、上記チケット秘密情報に関連して生成されていることを検証する手段とを有することを特徴とする電子チケット検証装置。

【請求項 6 1】 検証装置および証明装置を用いて行う権利証明方法において、上記証明装置は、少なくともチケット秘密情報と証明装置固有情報とから生成されたデジタル情報であるチケットと、自ら保有する証明装置固有情報とから証明情報を生成し、上記検証装置は、上記証明情報が上記チケット秘密情報に関連して生成されたことを検証して上記チケットに関連する権利の存在を証明する権利証明方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、チケットやカードの作成、発行および利用の技術に関する。

【0002】

【従来の技術】 乗車券、通行券、入場券、指定券、予約

券、回数券、定期券、商品券、プリペイドカード、ポイントカード、会員証、通行証、許可証などは、それを保持する者（以下では利用者と呼ぶ）がそれに応じた各々の権利を保持することを証明する。ここでは、これらをまとめてチケットと呼ぶ。一般にチケットは、利用者に権利を与える者もしくはその代理人（以下ではまとめて発行者と呼ぶ）が発行して、利用者が保持管理する。従来、チケットは、紙やプラスチックなどへ印刷やエンボス加工などの処理を施すことで実現されていた。

【0003】 このようなチケットをここでは紙チケットと呼ぶ。近年では、発行者が、利用者に与えた権利を特定できて、正しいチケットであることを検証できる、という機能を持つ電子チケットを実現する試みがなされている。電子情報は、作成が容易であり、通信回線を通して送信できるという特長を持つ。しかしながら、完全なコピーを簡単に作れるので、電子チケットを実現するには、偽造と複製による不正利用への対策が必要である。電子署名により偽造は防止できるが、複製の防止は困難である。このため、複製による不正利用を防止することが、電子チケットの実現にあたっての最大の課題となっている。

【0004】 従来、電子チケットは、チケットの利用時に正当な利用者が確認する第 1 の従来技術、発行者以外の者にチケットを複写する機会を与えない第 2 の従来技術、検証時の通信を公開できるように第 2 の従来技術を修正した第 3 の従来技術の、3 つの方法で実現されてきた。

【0005】 以下、各従来技術について順次説明する。

【0006】 第 1 の従来技術は、チケットの利用時に正当な利用者が確認する方法である。この方法では、正当な利用者であるかを確認するために必要な情報（利用者特定情報）と、与えた権利とを対応づける情報をチケットとして発行して、利用者が記録管理する。発行者以外の者が勝手にチケットを偽造できないようにするためには、発行者がチケットに電子署名を施す。電子署名のないチケットは、偽造されたものと判断される。

【0007】 不正に複写したチケットの利用を防止するため、利用者は、チケットを利用する時に、チケットとともに、自分が利用者特定情報に適合する正当な利用者であることを示す。利用者特定情報に適合していれば、対応する権利の行使が認められ、適合していなければ拒否される。利用者特定情報には、身元、顔写真などの身体的特徴、パスワードなどの知識の所有、などが利用できる。身元を利用する場合には、身分証明書などを提示させて確認した身元を利用できる。顔写真などの身体的特徴の場合には、利用者はそれを提示する。パスワードの場合には、そのパスワードを利用者が入力する。

【0008】 第 2 の従来技術は、発行者以外の者にチケットを複写する機会を与えない方法である。この方法では、利用者特定情報を用いる必要がないので、匿名性を



持ったチケットを実現できる。しかし、不正にチケットを複写した場合に、その複写したチケットの不正利用を防止する方法がないので、チケットの複写を直接防止する必要がある。このため、利用者が保持管理しているチケットを複写できないようにする機構と、発行時や検証時の通信からチケットが漏洩しない機構の両方を必要とする。前者の達成のため、利用者は、発行者以外の者が自由に内容を変更できない装置を所持して、その装置の中にチケットを記録する方法をとっている。後者の達成のため、盗聴できない通信方法をとっている。

【0009】この従来技術の一例が、特開平 8 - 1 4 7 5 0 0 号公報で開示されている。この方法では、利用者が携帯するチケット格納装置に、チケット発行者がチケットの内容に電子署名を加えたチケットを閉じ込めることで、電子チケットを実現している。電子署名をしているので偽造は困難である。チケット格納装置からチケットを取り出すのに特別な命令を必要とすることで、チケットを複写されることを防止している。この方法によれば、チケット発行者毎に異なる署名鍵を利用できるので、複数のチケット発行者が発行した複数のチケットを、単一の格納装置に格納できる。また、利用者に関する情報を知らなくても、チケットの署名の正当性を確認するだけで検証が可能である。

【0010】第3の従来技術は、検証時の通信を公開できるように第2の従来技術を修正した方法である。

【0011】この方法では、チケットを秘密情報として利用者の所持する装置（証明器）に複写できないように記録するのは第2の従来技術と同じであるが、検証の方法が異なる。まず、検証を行う検証器は、証明器に乱数などの繰り返し利用されない値（チャレンジ）を送る。証明器は、チケットである秘密情報を利用した演算をチャレンジに対して施して、得られた値（レスポンス）を検証器に送り返す。検証器は、秘密情報とチャレンジを利用してレスポンスが演算されたことを確認することで、利用者の正当性を認証する。チャレンジとレスポンスから秘密情報を求めることを計算量的に困難とすることで、検証器と証明器との通信を秘匿する必要がなくなる。

【0012】セキュリティ施設へのアクセス制御のための認証に目的が限定されているが、第3の従来技術と同様の機能を提供する方法が、特公平 6 - 5 2 5 1 8 号公報で開示されている。この方法では、第3の従来技術に加えて、検証者が利用者に対応する証明器の秘密情報を管理しなくてもよいという特徴を持つ。利用者は、第3の従来技術における証明器に相当する携帯用物体を携帯している。認証を行う通信では、認証を行う施設（検証器）は、利用者もしくは携帯用物体から識別番号を受け取り、この識別番号から携帯用物体に固有のシークレット・コードと呼ばれる秘密情報を計算する。この秘密情報を利用したチャレンジ・レスポンスを行って利用者を

認証するので、検証器は秘密情報を保持管理する必要がない。

【0013】

【従来の技術の問題点】現在紙チケットが果たしている役割を電子チケットが担うには、発行者が、利用者に与えた権利を特定できて、正しいチケットであることを検証できる、という機能だけでは不十分である。当事者間で争いが生じた時には第三者による調停が必要である。このため、紙チケットが果たしていた、権利を証明する機能が、電子チケットにも必要になる。

【0014】したがって、電子チケットには、次の3点の機能が必須である。第1点は、正当な権利を持たないものが、不当にチケットを利用することを防止する機能である。第2点は、利用者が自分の保持するチケットの正当性を確認できる機能である。第3点は、チケットに与えられた権利内容を第三者に証明する機能である。ただし、第3の機能は第2の機能を包含しているので、第1と第3の機能が実現されれば、チケットに必須の機能が満たされる。さらに、第4点として、利用者の匿名性を保証する機能が要請されることもある。

【0015】第1の従来技術では、利用する利用者特定情報に応じて、いくつかの機能が失われる。

【0016】利用者特定情報に利用者の身元を利用する方法では、発行時と検証時に利用者の身元が明らかになる。利用者特定情報に顔写真などの身体的特徴を利用する方法では直接身元が特定される訳ではないが、人物を特定するという意味で匿名性が失われている。いずれの方法にしても匿名性が失われるので、匿名性を有するチケット（第4の機能）が実現できない。

【0017】さらに、通信回線を利用した遠隔的な環境で身分を安全に証明する方法は実現されていないので、このような環境では第1の機能を提供できない。

【0018】第1の従来技術において、利用者特定情報にパスワードを利用する方法では、匿名性の問題は軽減されるが、パスワードを記憶する負荷を利用者にあたえる。また、利用者が故意にパスワードを漏洩させることを防止できないので、不正利用の危険が増し、チケットに必要な第1の機能が達成されていない。

【0019】第2の従来技術では、利用者が保管しているチケットを複写できなくするのに加えて、発行者がチケットの正当性を検証している時の通信の内容も機密にしている。これより2つの問題が生じる。第1の問題は、発行者以外の者はチケットを複写できないので、チケットの正当性を第三者に証明することが困難になることである。これは、チケットに必要な機能の第3が達成されていないことを示す。第2の問題は、チケットの発行時と検証時の通信の内容も機密に行うので、チケットの発行時と検証時にプライバシーなどの利用者の権利が侵害されていないことを証明できないことである。

【0020】特開平 8 - 1 4 7 5 0 0 号公報に開示され

た方法は第 2 の従来技術の一例であるから、上述の問題を有する。

【0021】第 3 の従来技術は、認証のために利用されるものであり、正当なチケットを保持しているか否か以外に情報を伝達しない。このため、有効期限などを示すことができず、単純なチケットしか表現できない。また、チケットを証明器に送信する方法が、第 3 の従来技術と同様に機密通信で行う必要があり、不当に利用者の情報を開示して利用者の権利を侵害していないことを証明できない。

【0022】特公平 6 - 5 2 5 1 8 号公報に開示されている方法は第 3 の従来技術の一例であるから、上述の問題を有する。

【0023】これまでに述べたように、従来の技術はいずれも、チケットに必要な第 1 の機能である不正利用を防止する機能を実現するために、第 2 および第 3 の機能である第三者に対するチケットの内容証明の機能や、第 4 の機能である利用者の匿名性を、犠牲にしている点に問題があった。

【0024】

【解決しようとする課題】そこで本発明は、上記の問題を解決するために、第 1 の機能として、偽造や複製などによる不正利用が非常に難しく、第 2 および第 3 の機能として、チケットの内容を第三者に証明できて、第 4 の機能として、チケットの利用時に利用者の匿名性が維持されるチケットの作成・発行・利用システムを実現することを課題とする。

【0025】

【課題を解決するための手段】本発明に係わる電子チケットシステムは、以下のチケット発行装置とチケット証明装置とチケット検証装置とからなる。チケットを発行するチケット発行装置は、チケットの特徴情報を保持する手段と、証明装置の固有情報を保持する手段と、チケットの特徴情報と証明装置の固有情報からチケットを計算する手段とを持つ。チケット証明装置は、チケット保持手段と、チケット検索手段と、固有情報保持手段と、内部状態保持手段と、証明手順実行手段と、検証装置との通信手段とを持つ。チケット検証装置は、検証手順実行手段と、証明装置との通信手段とを有する。

【0026】チケット発行装置は、チケットの特徴情報と証明器の固有情報とからチケットを発行する。証明装置は、チケット発行装置が発行したチケットを保持する。また、検証装置と通信手段を介して接続し、保持するチケットに対応する証明手順を実行することによって対話を行ない、証明を成功させることによってチケットの利用がなされる。証明手順実行手段は手順の実行において、検証装置から送信されたチケット識別子に対応するチケットを、検索手段を用いて検索し、対応するチケットが存在する場合には、そのチケットを用いて証明手順を実行する。証明手順の実行にあたっては固有情報保

持手段に保持された固有情報と内部状態保持手段に保持された内部情報を用いることができる。チケットの利用では、証明装置は特徴情報から決定されるチケットの有効性の証明と、チケットに対応する情報の更新や伝達が行なわれる。検証装置は、証明装置と通信手段を介して接続し、検証手順を実行することによって対話を行ない、対話の結果によって証明装置が有効なチケットを保持していることを検証する。チケットの検証では、検証装置は特徴情報から決定されるチケットの有効性の検証と、証明装置の保持するチケットに対応する情報の更新指示や獲得を行う。

【0027】

【発明の実施の態様】以下、本発明の詳細をつぎの順に説明する。

1. 実施例全体の概要 (図 1 2、図 2 8、図 2 9)

2. 第 1 の実施例

2. 1. 認証手法

2. 2. 簡単な対話プロトコル (図 1 3、図 1 9、図 2 0)

20 定期券型チケット

2. 3. 第 1 の対話プロトコル (図 1 4、図 1 9、図 2 1)

定期券型チケット (検証装置に時計)

2. 4. 第 2 の対話プロトコル (図 1 5、図 1 9、図 2 2)

メンバーズカード型チケット

2. 5. 第 3 の対話プロトコル (図 1 6、図 1 9、図 2 3)

回数券型チケット (使い捨て)

30 2. 6. 第 4 の対話プロトコル (図 1 6、図 1 9、図 2 4)

回数券型チケット (再充填可能)

2. 7. 第 5 の対話プロトコル (図 1 7、図 1 9、図 2 5)

スタンプカード型チケット

2. 8. 第 6 の対話プロトコル (図 1 8、図 1 9、図 2 6)

プリペイドカード型チケット (使い捨て)

2. 9. 第 7 の対話プロトコル (図 1 8、図 1 9、図 2 7)

プリペイドカード型チケット (再充填可能)

2. 10. 第 8 の対話プロトコル (図 1 6、図 1 9、図 2 4)

回数券型チケット

2. 11. 第 9 の対話プロトコル (図 1 8)

プリペイドカード型チケット

2. 12. 第 10 の対話プロトコル (図 1 8、図 1 9、図 2 7)

プリペイドカード型チケット

2. 13. 第 11 の対話プロトコル (とくになし)

複数プロトコルの実装

2. 1 4. 第 1 2 の対話プロトコル (図 1 9、図 3 1)  
チケット補助情報によるプロトコル付与

2. 1 5. 第 1 3 の対話プロトコル (図 3 0)

検証器の構成

3. 第 2 の実施例

3. 1. 認証手法

3. 2. 第 1 4 の対話プロトコル (図 1 3、図 1 9、図 2 0)

定期券型チケット

3. 3. 第 1 5 の対話プロトコル (図 3 2、図 1 9、図 3 3)

定期券型チケット

4. 第 3 の実施例 (図 5 ~ 図 9)

5. 第 4 の実施例 (図 4、図 5)

【0028】 [1. 実施例全体の概要]

(図 1、図 2、図 3、図 1 2、図 2 8、図 2 9) 図 1 は本発明の電子チケットシステムの構成図である。図 1 において、この発明の電子チケットシステムは、チケット作成・発行装置 1、チケット証明装置 2、およびチケット検証装置 3 を含んで構成されている。チケット作成・発行装置 1 はチケット作成手段 4 およびチケット発行手段 5 を有している。チケット作成手段 4 は、チケット作成依頼者 (チケットを受け取って対価を享受する者や、その代理人) のチケット作成依頼に基づいて、所定のサービスや物に対応するチケットの仕様を作成する。チケット発行手段 5 は、チケット発行依頼者 (チケットを示してサービス等の提供を受けたい者またはその代理人) のチケット発行依頼に基づいて、チケット識別子と証明器識別子とチケット仕様識別子とチケット付加情報を入力として、対応するチケットを発行する。

【0029】チケット証明装置 2 は、チケット発行手段 5 の発行したチケットを保持し、チケット検証装置 3 と通信を行ないチケットの保有を証明する。チケット検証装置 3 は、チケット作成手段 4 の作成したチケット識別子とチケット検証手順を保持し、チケット証明装置 2 と通信を行ないチケットの検証を行なう。なお、以下では、チケット作成・発行装置 1、チケット証明装置 2 およびチケット検証装置 3 をそれぞれチケット作成・発行器、チケット証明器およびチケット検証器または単に作成・発行器、証明器および検証器と呼ぶことがある。

【0030】図 2 および図 3 はチケット作成・発行装置 1 の構成を全体として示している。また、図 1 2 はチケット証明装置 2 およびチケット検証装置 3 の構成を全体として示している。なお、図 2 および図 3 はほぼ同一の構成を示している。ただし、図 2 が一般的な公開暗号系を認証に用いる例を説明するのに対して、図 3 は RSA 公開暗号系を認証に用いる例を説明している。

【0031】図 2 において、チケット作成・発行装置 1 は、チケット作成部 (手段) 4、チケット発行部 (手

段) 5、チケット原型データベース 6 および証明器固有情報データベース 7 を有している。図 3 においては、さらに、チケット仕様データベース 8 が設けられている。チケット作成・発行装置 1 の詳細 (動作) については第 3 の実施例および第 4 の実施例を参照して後述する。

【0032】図 1 2 において、チケット検証装置 3 は、検証手順実行部 1 1 1 および通信部 1 1 2 を有しており、また、チケット証明装置 2 は、チケット保持部 1 2 1、チケット検索部 1 2 2、固有情報保持部 1 2 3、内部状態保持部 1 2 4、証明手順実行部 1 2 5 および通信部 1 2 6 を有している。

【0033】図 2 9 はチケット証明装置 2 の証明手順実行部 1 2 5 の詳細な構成を示しており、また、図 2 8 はチケット検証装置 3 の検証手順実行部 1 1 1 の詳細な構成を示している。図 2 8 および図 2 9 に示すように、本実施例では、証明装置 2 の証明手順実行部 1 2 5 は、送信部 2 9 1、受信部 2 9 2、第 1 の演算部 2 9 3、第 2 の演算部 2 9 4、正当性検証部 2 9 5、認証情報生成部 2 9 6、認証情報保持部 2 9 7、第 2 の認証情報保持部 2 9 8、情報保持部 2 9 9、出力情報保持部 2 9 1 0、入力情報保持部 2 9 1 1、制御部 2 9 1 2 とから構成されている。

【0034】検証装置 3 の検証手順実行部 1 1 1 は、送信部 2 8 1、受信部 2 8 2、第 1 の演算部 2 8 3、第 2 の演算部 2 8 4、正当性検証部 2 8 5、認証情報生成部 2 8 6、認証情報保持部 2 8 7、チケット識別子保持部 2 8 8、情報保持部 2 8 9、出力情報保持部 2 8 1 0、入力情報保持部 2 8 1 1、出力部 2 8 1 2、入力部 2 8 1 3、利用証情報保持部 2 8 1 4 とから構成される。

【0035】以下の例示において各手順実行部を構成する手段の中から必要なものを用いて証明手順・検証手順を実行するものとする。

【0036】 [2. 第 1 の実施例] まず本発明の第 1 の実施例について説明する。

【2. 1. 認証手法】チケットはチケットの特徴情報と証明器 2 の固有情報とからチケット発行装置によって算出される。チケットの特徴情報が RSA 公開鍵暗号系における公開情報と秘密情報、つまり、 $p$ 、 $q$  を相異なる奇素数とし、

【0037】

【数 1 0】

$n = p q$ 、 $\lambda(n) = \text{lcm}(p-1, q-1)$ 、  
(ここで  $\text{lcm}$  は最小公倍数を表す)

【0038】

【数 1 1】  $E D \equiv 1 \pmod{\lambda(n)}$

が満たされるとき、 $(n, E)$  を公開情報とし、 $D$  を対応する秘密情報とする場合について、実現できるチケットの証明方法について詳述する。

【0039】チケットはチケット特徴情報  $D$  と証明器固有情報  $d$  とチケット付加情報  $L$  より計算されるデータ

であり、証明器 2 が  $(C, n, t, L)$  に対して証明器固有情報  $d_s$  を用いて  $r(C, n, t, L) = C^r \bmod n$  が計算できるように構成する。

【0040】例えば、 $d_s$  をある暗号系の復号鍵とし、 $E_s$  を  $d_s$  に対応する暗号化とし、 $H$  を一方向性関数としたとき、

【0041】

【数 12】

$t := (E_s(D), H(d_s || D || L))$

のように定めることができる。(ここで  $||$  はビット列の連結である。)

チケットを (1) として定義すると、チケットを用いた秘密の特徴情報  $D$  による符号化  $C^r \bmod n$  は、入力  $(C, n, t, L)$  に対して証明装置の固有情報  $d_s$  によって  $E_s(D)$  を復号して証明装置中で  $D$  を回復し、その値を用いて一方向性関数の値をチケットと比較することによって  $L$  の値の正当性を確認し、回復された  $D$  の値を用いて証明装置内で  $C^r \bmod n$  を計算するようにすれば良い。

【0042】また、 $d_s$  を一方向性関数として、

【0043】

【数 12】  $t := D - d_s(L, n)$

と定めることもできる。

【0044】チケットを上式として定義すると、入力  $(C, n, t, L)$  に対して  $D$  による符号化  $C^r \bmod n$  は、 $C^r C^{t(L,n)} \bmod n$  を計算することによって行なうこともできる。このチケットにおいては、 $L$  の値の完全性も  $D$  の値も証明器 2 の秘密計算を行なう部分ではチケット  $t$  もしくは公開情報  $E$  を入力しない限り確認できず、また、チケット  $t$  を証明器 2 の秘密計算を行なう部分に入力せずに秘密情報に対応する符号化が計算できるという特徴がある。

【0045】証明器 2 の固有情報  $d_s$  と  $(C, n, t, L)$  に対して  $C^r \bmod n$  を計算する手段の少なくとも一部は耐タンパー性を有する容器に保護することが望ましい。

【0046】なお、以下の証明手順の例示において図 19 におけるステップ 194 以外は全てに共通する。したがって、ステップ 194 の詳細な手順 (Prover で示す) を重点的に説明する。

【0047】【2. 2. 簡単な対話プロトコル】

(証明器 2 が時計を持つ定期券型のチケット、図 13、図 19、図 20) 以下、検証器 3 と証明器 2 との対話の簡単な例をあげて説明する。以下の例では証明器 2 の内部情報として現在時刻を持つものとする。なお、以下では、検証手順と証明手順とをまとめて対話プロトコルと呼ぶことにする。

【0048】簡単な対話の例における検証器 3 の構成を図 12 および図 28 に示し、手順を図 13 に従って説明する。証明器 2 の構成を図 12 および図 29 に示し、手

順を図 19 に従って説明する。

【0049】検証器 3 は、認証情報生成部 286 でチャレンジ  $C$  を生成して、認証情報保持部 287 に記録する (ステップ 131)。この  $C$  は、過去に利用した値を再び利用しないことが求められる。特に  $C$  は乱数であることが望ましい。認証情報保持部 287 に記録された  $C$  と、識別子保持部 288 に保持されている検証しようとするチケットの識別子  $n$  とをまとめて、送信部 281 より証明器 2 へ送信する (ステップ 132)。

【0050】証明器 2 は、検証器 3 から送信された  $(C, n)$  を受信部 292 で受信して、情報保持部 299 に記録する (ステップ 191)。チケット探索部 122 は受信した  $n$  に対応するチケットをチケット保持部 121 から探して、チケットを持っているかを判定する (ステップ 192)。ただし、1 種類のチケットしか扱わないような本発明の適用場面では、 $n$  に対応するチケットを探す手順は不要になり、チケットを持っているかを判定するだけである。この場合には、ステップ 132 において検証器 3 から  $(C, n)$  を送る必要はなくなり、 $C$  だけ送れば十分である。さらにチケットを持っていることが保証されている場合には、持っているかの判定の手順 (ステップ 192) およびステップ 197 も不要になる。ステップ 192 の判定の結果として対応するチケットを持たない場合には、レスポンス  $R$  にチケットを持たないことを意味する値 (この場合は 0) を設定して、情報保持部 299 に記録する (ステップ 197)。ステップ 192 の判定の結果として対応するチケットを持つ場合には、チケット  $t$ 、証明器 2 の手順  $Prover$ 、チケット付加情報  $L$  を制御部 2912 内にセットする (ステップ 193)。

【0051】ステップ 193 が実行されたら、ステップ 194 を実施する。この対話の例におけるステップ 194 の詳細な手順を図 20 に従って説明する。内部状態保持部 124 の第 2 の内部状態保持部から読み出したその時の時刻  $time$  と、 $L$  に記述されている有効期限とを比較して、チケットがその時点で有効であるか判定する (ステップ 201)。この判定には、有効期限として終了時刻のみを記述している場合には、 $time$  がその終了時刻に達していれば無効であり、達していなければ有効であると判定できる。有効期限として開始時刻および終了時刻を記述している場合には、 $time$  がその開始時刻と終了時刻の間になれば無効であり、間になれば有効であると判定できる。チケットを有効であると判定した場合には、第 1 の演算部 293 において  $R$  を、 $R := C^r \bmod n$  のように計算して、情報保持部 299 に記録する (ステップ 202)。特に  $R$  のこの計算を、証明器 2 の中の第 1 の演算部 293 ですべて計算してもよいが、チケット  $t$  が  $t := D - d_s(L, n)$  のように構成されている場合には、 $C^r \bmod n$  の計算は  $C^r C^{t(L,n)} \bmod n$  のようにも計算できるの

で、 $C^t \bmod n$  を証明器 2 の外で計算して、証明器 2 の中の第 1 の演算部 293 で計算した  $C^{t'}$   $\bmod n$  とを証明器 2 の外で掛け合わせても計算できる。証明器 2 の計算速度が遅い場合には、このような方法も有効になる。

【0052】ステップ 201 においてチケットを無効であると判定した場合には、必要であるならばチケットをチケット保持部 121 から削除して（ステップ 203）、 $R$  にチケットが有効期間でなかったことを意味する値（この例では 1）を設定して、情報保持部 299 に 10 記録する（ステップ 204）。ここまでがこの対話の例におけるステップ 194 の詳細な手順である。

【0053】ステップ 194 が実行されたら、ステップ 193 でセットされた  $t$ 、 $Prover$ 、 $L$  を制御部 2912 から解除する（ステップ 195）。ステップ 195 もしくはステップ 197 が実行されたら、 $R$  を送信部 291 より検証器 3 へ送信する（ステップ 196）。

#### 検証器

公開情報:  $(n, E)$

出力: '有効' もしくは '無効'

```

C := rand
send (C, n)
receive R
R := RE mod n
if C = R
    output '有効'
else
    output '無効'

```

Prover

```

if time < L
    R := CD mod n
else
    R := 1

```

【0058】【2.3. 第 1 の対話プロトコル】

（検証器 3 が時計を持つ定期券型のチケット、図 14、図 19、図 21）検証器 3 と証明器 2 との種々の対話の方式を以下順次列挙して説明する。先に説明した構成の基に、検証の手順と証明の手順を変更することにより、異なる機能性を持つチケットを同一の構成によって実現できる。

【0059】まず、第 1 の対話プロトコルについて説明する。第 1 の対話プロトコルでは、検証器 3 の認証情報は単なる乱数ではなく、証明器 2 の証明情報生成の条件が、送信された認証情報とチケット発行時に固定された

【0054】検証器 3 は、受信部 282 において証明器 2 から送信された  $R$  を受信して、情報保持部 289 に記録する（ステップ 133）。 $R := R^t \bmod n$  を第 1 の演算部 283 で計算して、その計算結果が認証情報保持部 287 で記録している  $C$  と一致するかを、正当性検証部 285 で判定する（ステップ 134）。一致すると判定された場合は証明器 2 が有効なチケットを持っていることを示すので、「有効」を意味する出力を出力部 2812 より出力する。一致しないと判定された場合は証明器 2 が有効なチケットを持っていることが示されなかったので、「無効」を意味する出力を出力部 2812 より出力する。

【0055】以上が対話の簡単な例である。

【0056】対話手順を簡略に記述すると、以下のとおりである。

【0057】

【表 1】

40 情報  $L$  との関係に依存するものである。

【0060】例えば、検証器 3 が現在時刻を表現する情報を発行する手段を持ち、時間情報を認証情報に埋め込み、 $L$  を有効期限を表現する情報とすると、証明器 2 に時計機能を保持することなく時間制限型のチケットを実現できる。 $L$  のビット長を  $|L|$  で表す。

【0061】第 1 の対話プロトコルの検証器 3 の手順を図 14 に、証明器 2 の手順を図 19 にそれぞれ従って説明する。

【0062】検証器 3 は、認証情報生成部 286 で乱数  $r$  を生成して（ステップ 141）、さらに、 $r$  とその時

の時刻  $time$  とを結合してチャレンジ  $C$  を生成して、認証情報保持部 287 に記録する (ステップ 142)。例えば、 $r$  と  $time$  の結合は、 $C := r || time$  のように実現すればよい。識別子保持部 288 に記録されている検証しようとするチケットの識別子  $n$  と  $C$  とを合わせて、送信部 281 より証明器 2 へ送信する (ステップ 143)。

【0063】証明器 2 の処理の流れはステップ 193 までは最初の対話例と同じである。証明器 2 は、検証器 3 から送信された ( $C, n$ ) を受信部 292 で受信して、情報保持部 299 に記録する (ステップ 191)。チケット探索部 122 が受信した  $n$  に対応するチケットをチケット保持部 121 から探して、チケットを持っているかを判定する (ステップ 192)。対応するチケットを持たない場合には、レスポンス  $R$  に 0 を設定して、情報保持部 299 に記録する (ステップ 197)。対応するチケットを持つ場合には、チケット  $t$ 、証明器 2 の手順  $Prover$ 、チケット付加情報  $L$  をセットする (ステップ 193)。

【0064】ステップ 193 が実行されたら、ステップ 194 を実施する。第 1 の対話プロトコルにおけるステップ 194 の詳細な手順を図 21 に示す。 $C$  から  $time$  を抽出する (ステップ 211)。この抽出には、 $C$  から決められた長さの下位の桁を取り出せばよい。

【0065】例えば、 $C$  が 2 進数表現されていて、 $time$  の長さを  $|L|$  ビットと表現するならば、 $time := C \bmod 2^{|L|}$  によって取り出すことができる。ステップ 211 で  $time$  を取り出したら、 $L$  に記述されている制限事項である有効期限と比較してチケットがその時点で有効であるかを判定する (ステップ 212)。この判定は、最初の対話例のステップ 201 で説明した方法と同様である。ステップ 212 の結果としてチケットが有効であると判定した場合には、証明器 2 は  $R$  として、 $R := C^D \bmod n$  を第 1 の演算部 293 で計算して、情報保持部 299 に記録する (ステップ 213)。ステップ 212 の結果としてチケットが無効であると判定した場合には、必要ならばチケット保持部 121 からチケットを削除して、 $R$  にチケットが有効期間でなかったことを意味する値 (この場合では 1) を設定して、情報保持部 299 に記録する (ステップ 214)。ここまでの第 1 の対話プロトコルにおけるステップ 194 の詳細な手順である。

【0066】ステップ 194 が実行されたら、ステップ 193 でセットされた  $t$ 、 $Prover$ 、 $L$  を解除する (ステップ 195)。ステップ 195 もしくはステップ 197 が実行されたら、送信部 291 から検証器 3 へ  $R$  を送信する (ステップ 196)。

【0067】検証器 3 は、証明器 2 から送信された  $R$  を受信部 282 に受信して、情報保持部 289 に記録する (ステップ 144)。 $R := R^E \bmod n$  を第 1 の

演算部 283 で計算して、この演算結果が認証情報保持部 287 に記録されている  $C$  と一致するかを、正当性検証部 285 で判定する (ステップ 145)。一致する場合は証明器 2 が有効なチケットを持っていることが示されたので、「有効」を意味する出力を出力部 2812 から出力する。一致しない場合は証明器 2 が有効なチケットを持つことが示されなかったので、「無効」を意味する出力を出力部 2812 から出力する。

【0068】以上が第 1 の対話プロトコルである。証明器 2 が時計を持たなくても、最初の対話例と同じ機能を実現している。本プロトコルを、検証器が「有効」を出力したらゲートを開け、「無効」を出力したら、ゲートを閉ざすように適用することで、有効期限付きの通行証や定期券の機能を実現できる。

【0069】以上の対話手順を簡略に記述すると、以下のとおりである。

【0070】

【表 2】

#### 検証器

公開情報: ( $n, E$ )

出力: '有効' もしくは '無効'

$C := rand || time$

send ( $C, n$ )

receive  $R$

$R := R^E \bmod n$

if  $C = R$

output '有効'

else

output '無効'

#### Prover

if  $C \bmod 2^{|L|} < L$

$R := C^D \bmod n$

else

$R := 1$

【0071】【2. 4. 第 2 の対話プロトコル】

(メンバーズカード型のチケット、図 15、図 19、図 22) 第 2 の対話プロトコルでは、証明手順において、証明器 2 が送信する証明情報は、認証情報にチケット発行時に関係付けられた固定的な情報  $L$  を添加したものを、チケットの特徴情報に基づいて符号化したものとする。また、検証手順において、証明情報が認証情報に対応することの検証と付加的に得られる情報  $L$  の導出を行なう。

【0072】このプロトコルでは証明器 2 から検証器 3

に対して、チケット発行時に関係付けられた定数が伝達される。

【0073】第2の対話プロトコルの、検証器3の手順を図15に従って説明し、証明器2の手順を図19に従って説明する。

【0074】検証器3はチャレンジCを認証情報生成部286で生成して、認証情報保持部287に記録する(ステップ151)。検証しようとするチケットの識別子nと生成したCを合わせて、送信部281より証明器2へ送信する(ステップ152)。

【0075】証明器2の処理の流れは、最初の対話例とステップ193まで同じである。証明器2は、検証器3から送信された(C, n)を受信部292で受信して、情報保持部299に記録する(ステップ191)。チケット探索部122は受信したnに対応するチケットをチケット保持部121から探して、チケットを持っているかどうかを判定する(ステップ192)。判定の結果として対応するチケットを持たない場合には、レスポンスRに0を設定して、情報保持部299に記録する(ステップ197)。判定の結果として対応するチケットを持つ場合には、チケットt、証明器2の手順Prover、チケット付加情報Lをセットする(ステップ193)。

【0076】ステップ193が実行されたら、ステップ194を実行する。第2の対話プロトコルにおけるステップ194の手順の詳細な手順を図22に従って説明する。Lから取り出した、検証器3に送出するメッセージMと、Cとを結合して、情報保持部299に記録する(ステップ221)。CとMの結合の方法は、 $C := C || M$ によって実現できる。結合したCを使って、第1の演算部283において $R := C^0 \bmod n$ を計算して、情報保持部299に記録する(ステップ222)。ここまでの、第2の対話プロトコルにおけるステップ194の詳細な手順である。

【0077】ステップ194が実行されたら、ステップ193でセットされたt、Prover、Lを解除する(ステップ195)。ステップ195もしくはステップ197が実行されたら、Rを送信部291より検証器3へ送信する(ステップ196)。

【0078】検証器3は、証明器2から送信されたRを受信部282で受信して、情報保持部289に記録する(ステップ153)。 $R := R^1 \bmod n$ を第1の演算部283で計算して(ステップ154)、この計算されたRの上位の桁が、認証情報保持部287に記録されているCと一致することを、正当性検証部285で判定する(ステップ155)。一致していればRの下位の桁よりMを取り出して(ステップ156)、出力部2812より出力する。一致していなければ証明器2が有効なチケットを持つことが示されなかったので、「無効」を意味する出力を出力部2812より出力する。

【0079】以上が第2の対話プロトコルである。本プロトコルによると、証明器2はチケットを持つことを証明すると同時に、改竄を検知できるようにメッセージを検証器3へ伝達できる。例えば、メッセージを会員番号として本プロトコルを適用することで、会員であることを証明すると同時に、会員番号を伝達する会員証が実現される。

【0080】

【表3】

### 検証器

公開情報:  $(n, E)$

出力:  $M (= L)$  もしくは '無効'

```

C := rand
send (C, n)
receive R
R := R^E mod n
if R = C || M
    output M
else
    output '無効'

```

Prover

$M := L$

$R := (C || M)^D \bmod n$

【0081】[2. 5. 第3の対話プロトコル]

(使い捨ての回数券型のチケット、図16、図19、図23)第3の対話プロトコルでは、チケットに対して証明器2が可変な内部状態を持ち、チケット利用において検証器3が内部状態の更新を行なう。内部状態の更新を行ないうる検証器3は、それを証明する秘密の特徴情報を持つ。この特徴情報を持つ検証器3を特権を持つ検証器3と呼ぶ。

【0082】また、その特徴情報を持たない検証器3との対話においては、内部状態の更新を回避してチケットの有効性を検証することができる。

【0083】例えば、証明器2が持つ内部状態を度数情報とする。検証器3側で把握することなく、特権を持つ検証器3との対話の回数を制限する機構を実現する。

【0084】検証器3の特権を保証する特徴情報を $(\delta, \nu)$ として、検証器3の特徴情報に対応する公開情報を $(\epsilon, \nu)$ とする。ただし、 $\epsilon \delta \equiv 1 \bmod \lambda(\nu)$ である。利用するチケット補助情報Lには、検証器3の特徴情報の公開情報 $(\nu, \epsilon)$ と、内部状態であるカウンタの上限値iが含まれている。例えば、 $L := \nu || \epsilon || i$ のように構成しておき、それぞれの情報の長さが決められていれば、Lからそれぞれの情報を

取り出すことができる。第3の対話プロトコルの検証器3の手順を図16に従って説明し、証明器2の手順を図19に従って説明する。

【0085】検証器3は、認証情報生成部286でチャレンジCを生成して、認証情報保持部287に記録する(ステップ161)。検証しようとするチケットの識別子nと生成したCを、まとめて送信部281より証明器2へ送信する(ステップ162)。

【0086】証明器2の処理の流れはステップ193までは最初の対話例と同じである。証明器2は、検証器3から送信された(C, n)を受信部292で受信して、情報保持部299に記録する(ステップ191)。チケット探索部122は受信したnに対応するチケットをチケット保持部121から探して、チケットを持っているかどうかを判定する(ステップ192)。対応するチケットを持たない場合には、レスポンスRに0を設定して、情報保持部299に記録する(ステップ197)。対応するチケットを持つ場合には、チケットt、証明器2の手順Prover<sub>i</sub>、チケット付加情報Lをセットする(ステップ193)。Prover<sub>i</sub>のセットによ

【0087】ステップ193が実行されたら、ステップ194を実行する。第3の対話プロトコルにおけるステップ194の詳細な手順を図23に示す。認証情報生成部296でチャレンジxを生成して、第2の認証情報保持部298に記録する(ステップ231)。xは、これまで示した最初の対話例におけるCの生成と同じ方法で生成できる。生成したxを送信部291から検証器3へ送信する(ステップ232)。

【0088】検証器3は、xを受信部282で受信して、情報保持部289に記録する(ステップ163)。ただし、xとして0を受信した場合は、証明器2がチケットを持っていないくて、Rとして0を送ったことを意味するので、「無効」を意味する出力を出力部2812から出力して、対話プロトコルを終了する。第2の演算部284においてレスポンスρを、

【0089】

【数14】

$$\rho := x^e \bmod \nu$$

により計算する(ステップ164)。計算したρを送信部281より証明器2へ送信する(ステップ165)。

【0090】証明器2は、ρを受信部292で受信して、情報保持部299に記録する(ステップ233)。第2の演算部294で

【0091】

【数15】

$$\rho := \rho^e \bmod \nu$$

を計算する。第2の認証情報保持部298に記録されているxとρが、一致するか判定する(ステップ234)。判定の結果として一致しない場合には、メッセー

ジMに1を設定して、情報保持部299に記録する(ステップ239)。判定の結果として一致する場合には、Mに0を設定して、情報保持部299に記録して(ステップ235)、内部状態保持部124の第2の内部状態保持部に確保されているカウンタiの値をインクリメントする(ステップ236)。ステップ236もしくはステップ239が実行されたら、iの値をLより得られた上限値Iと比較する(ステップ237)。ステップ237の比較の結果として、iの値がI以下の場合

【0092】なお、上の説明ではiが初期値0に設定された後は、検証に成功する度にインクリメントしてIと大小を比較しているが、iの初期値をIに設定して、検証に成功するたびにデクリメントして負の値になるか判定する方法でも同様のことが実現できる。

【0093】ステップ194が実行されたら、ステップ193でセットされたt、Prover<sub>i</sub>、Lを解除する(ステップ195)。ステップ195もしくはステップ197が実行されたら、送信部291から検証器3へRを送信する(ステップ196)。

【0094】検証器3は、証明器2から送信されたRを受信部282に受信して、情報保持部289に記録する(ステップ166)。R := R<sup>t</sup> mod nを第1の演算部283で計算する(ステップ167)。この計算結果の上位の桁が、認証情報保持部287に記録されているCと一致するかを、正当性検証部285で判定する(ステップ168)。一致する場合は証明器2が有効なチケットを持っていることが示されたので、Rの下位の桁より取り出したMを、証明器2から受け取った情報として取り出して(ステップ169)、出力部2812から出力する。一致しない場合は証明器2が有効なチケットを持つことが示されなかったので、「無効」を意味する出力を出力部2812から出力する。

【0095】以上が第3の対話プロトコルである。特権を持つ検証器3は決められた回数だけ、チケットの検証ができる。また、特権を持たない検証器3でも、レスポンスρとして適当な値を返すことで、チケットの有効性を検証できる。例えば、検証器3の出力が0の時だけサービスを提供して、それ以外の値の時に提供しないように本プロトコルを適用すると、回数券の機能を実現できる。



【 0 0 9 6 】

【 表 4 】

**検証器**公開情報:  $(n, E)$ 出力:  $M \in \{0(\text{有効: 対特権検証器}), 1(\text{有効: 対一般の検証器})\}$  もしくは '無効'特権を保証する特徴情報:  $(\delta, \nu)$ , ただし  $\epsilon\delta \equiv 1 \pmod{\lambda(\nu)}$ 

```

C := rand
send (C, n)
receive  $\chi$ 
 $\rho := \chi^\delta \pmod{\nu}$ 
send  $\rho$ 
receive R
 $R := R^E \pmod{n}$ 
if  $R = C || M$ 
    output M
else
    output '無効'

```

**Prover**

```

 $\nu || \epsilon || i := L$ 
 $\chi := \text{rand}$ 
send  $\chi$ 
receive  $\rho$ 
 $\rho := \rho^\epsilon \pmod{\nu}$ 
if  $\rho = \chi$ 
     $i_n := i_n + 1$ 
     $M := 0$ 
else
     $M := 1$ 
if  $i_n \leq i$ 
     $R := (C || M)^D \pmod{n}$ 
else
    free  $i_n$ 
    delete t
     $R := 1$ 

```

【 0 0 9 7 】 【 2 . 6 . 第 4 の対話プロトコル】

(再充填可能な回数券型のチケット、図 1 6、図 1 9、図 2 4) 第 4 の対話プロトコルでは、第 3 の対話プロトコルにおけると同様にレスポンスの生成回数を制限する機構を実現する。本対話プロトコルでは、さらに、特権的な検証者は消費された利用回数を充当することができる。

【 0 0 9 8 】 このプロトコルでは検証器 3 から証明器 2 に対して、検証器 3 が特権的であることと検証器 3 の 1 ビットの指示 (対応する内部状態に対しての 2 通りの更新指示の選択: 度数の消費と度数の充填) が伝達され

40 る。

【 0 0 9 9 】 これによってチケットの発行をチケット作成・発行装置が一度行なえば、そのチケットが無効になった場合、チケット作成・発行装置による新たなチケット発行によらず、特権を持つ検証者と対話を行なうことによって有効性を回復する。

【 0 1 0 0 】 検証器 3 の特権を保証する特徴情報の  $(\delta, \nu)$  および公開情報の  $(\epsilon, \nu)$ 、チケット補助情報は第 3 の対話プロトコルと同じである。第 4 の対話プロトコルの検証器 3 の手順を図 1 6 に従って説明し、証明器 2 の手順を図 1 9 に従って説明する。ただ

し、対話プロトコルに先立って、度数の消費を実行するのか、度数の充填を実行するのかを、検証器 3 の入力部 2813 より入力されて、入力情報保持部 2811 に記録されているとする。

【0101】検証器 3 は認証情報生成部 286 でチャレンジ C を生成して、認証情報保持部 287 に記録する（ステップ 161）。検証しようとするチケットの識別子 n と生成した C を、まとめて送信部 281 より証明器 2 へ送信する（ステップ 162）。

【0102】証明器 2 は、検証器 3 から送信された (C, n) を受信部 292 で受信して、情報保持部 299 に記録する（ステップ 191）。チケット探索部 122 は受信した n に対応するチケットをチケット保持部 121 から探して、チケットを持っているかどうかを判定する（ステップ 192）。対応するチケットを持たない場合には、レスポンス R に 0 を設定して、情報保持部 299 に記録する（ステップ 197）。対応するチケットを持つ場合には、チケット t、証明器 2 の手順 Prover、チケット付加情報 L をセットする（ステップ 193）。

【0103】ステップ 193 が実行されたら、ステップ 194 を実行する。第 4 の対話プロトコルにおけるステップ 194 の詳細な手順を図 24 に従って説明する。認証情報生成部 296 でチャレンジ x を生成して、第 2 の認証情報保持部 298 に記録する（ステップ 241）。生成した x を送信部 291 から検証器 3 へ送信する（ステップ 242）。

【0104】検証器 3 は、x を受信部 282 で受信して、情報保持部 289 に記録する（ステップ 163）。x として 0 を受信した場合は、証明器 2 がチケットを持

っていないくて、R として 0 を送ったことを意味するので、「無効」を意味する出力を出力部 2812 から出力して、対話プロトコルを終了する。次に、レスポンス  $\rho$  を計算する（ステップ 164）。まず、第 2 の演算部 284 においてレスポンス  $\rho$  を、

【0105】  
【数 16】

$$\rho := x^{\delta} \bmod \nu$$

のように計算する。チケットの度数の充填を行いたい場合にはさらに、第 2 の演算部 284 において、

【0106】

【数 17】

$$\rho := \rho^{\delta} \bmod \nu$$

を計算する。ステップ 164 における  $\rho$  の計算は、チケットの度数の消費を行いたい場合には  $\mu := 1$  として、チケットの度数の充填を行いたい場合には  $\mu := 2$  として、

【0107】

【数 18】

$$\rho := x^{\delta \mu} \bmod \nu$$

を計算しても同様である。ステップ 164 で計算した  $\rho$  を送信部 281 より証明器 2 へ送信する（ステップ 165）。

【0108】証明器 2 は、 $\rho$  を受信部 292 で受信して、情報保持部 299 に記録する（ステップ 243）。第 2 の演算部 294 で

【0109】

【数 19】

$$\rho := \rho^{\delta} \bmod \nu$$

10 を計算して、第 2 の認証情報保持部 298 に記録されている  $x$  と  $\rho$  が、一致するか判定する（ステップ 244）。ステップ 244 の判定の結果が一致する場合には、M に 0 を設定して情報保持部 299 に記録して、内部状態保持部 124 に確保されているカウンタ  $i$  の値をインクリメントする（ステップ 245）。ステップ 244 の判定の結果が一致しない場合には、第 2 の演算部 294 で

【0110】

【数 20】

$$\rho := \rho^{\delta} \bmod \nu$$

を計算して、第 2 の認証情報保持部 298 に記録されている  $x$  と  $\rho$  が、一致するか判定する（ステップ 248）。ステップ 248 の判定の結果が一致する場合には、M に 0 を設定して情報保持部 299 に記録して、内部状態保持部 124 の第 2 の内部状態保持部に確保されているカウンタ  $i$  の値を 0 に設定する（ステップ 249）。ステップ 248 の判定の結果が一致しない場合には、メッセージ M に 1 を設定して、情報保持部 299 に記録する（ステップ 2411）。ステップ 245 もしくはステップ 249、ステップ 2411 が実行されたら、 $i$  の値を  $L$  より得られた上限値  $l$  と比較する（ステップ 247）。ステップ 247 の比較の結果として、 $i$  の値が  $l$  以下の場合は、第 1 の演算部 293 で  $R := (C || M)^{\delta} \bmod n$  を計算して、情報保持部 299 に記録する（ステップ 248）。ステップ 247 の比較の結果として、カウンタ  $i$  が  $l$  よりも大きい場合は、R の値を 1 に設定して情報保持部 299 に記録する（ステップ 2410）。ここまでが第 4 の対話プロトコルにおけるステップ 194 の詳細な手順である。

40 【0111】ステップ 194 が実行されたら、ステップ 193 でセットされた t、Prover、L を解除する（ステップ 195）。ステップ 195 もしくはステップ 197 が実行されたら、送信部 291 から検証器 3 へ R を送信する（ステップ 196）。

【0112】検証器 3 は、証明器 2 から送信された R を受信部 282 に受信して、情報保持部 289 に記録する（ステップ 166）。 $R := R^{\delta} \bmod n$  を第 1 の演算部 283 で計算する（ステップ 167）。この計算結果の上位の桁が、認証情報保持部 287 に記録されている C と一致するかを、正当性検証部 285 で判定する

(ステップ168)。一致する場合は証明器2が有効なチケットを持っていることが示されたので、Rの下位の桁より取り出したMを、証明器2から受け取った情報として取り出して(ステップ169)、出力部2812から出力する。一致しない場合は証明器2が有効なチケットを持つことが示されなかったので、「無効」を意味する出力を出力部2812から出力する。

【0113】以上が第4の対話プロトコルである。第4の対話プロトコルと同様の機能を提供する変形例とし

検証器公開情報:  $(n, E)$

入力:  $\mu \in \{1(\text{回数の消費指示}), 2(\text{回数の充填指示})\}$

出力:  $M \in \{0(\text{有効: 対特権検証器}), 1(\text{有効: 対一般の検証器})\}$  もしくは '無効'

特権保証特徴情報:  $(\delta, \nu)$

```

C := rand
send (C, n)
receive  $\chi$ 
 $\rho := \chi^E \bmod \nu$ 
send  $\rho$ 
receive R
 $R := R^E \bmod n$ 
if  $R = C || M$ 
  output M
else
  output '無効'

```

```

Prover
 $\nu || \epsilon || i := L$ 
 $\chi := \text{rand}$ 
send  $\chi$ 
receive  $\rho$ 
 $\rho := \rho^E \bmod \nu$ 
if  $\rho = \chi$ 
   $i_n := i_n + 1$ 
   $M := 0$ 
else
   $\rho := \rho^E \bmod \nu$ 
  if  $\rho = \chi$ 
     $i_n := 0$ 
     $M := 0$ 
  else
     $M := 1$ 
if  $i_n \leq i$ 
   $R := (C || M)^D \bmod n$ 
else
   $R := 1$ 

```

て、 $i$ の初期値を1に設定して、ステップ245でインクリメントの代わりにデクリメントして、ステップ246で負の値になるか判定する方法も実現できる。この変形例では、ステップ249の度数の充填時に $i$ を1に設定する。さらに別の変形例として、ステップ249の度数の充填時に $i$ に1を加える方法もある。

【0114】

【表5】

【0115】 [2. 7. 第5の対話プロトコル]

(スタンプカード型チケット、図17、図19、図25) 第5の対話プロトコルでは、特権を持つ検証者に対して生成したレスポンスの回数が、チケット発行時に割り付けられたある一定回数に達する都度、そのことを検証者に通知する機構を実現する。

【0116】 また、一般的な検証者に対してもチケットの有効性を確認することが可能である。

【0117】 検証器3の特権を保証する特徴情報の

( $\delta$ ,  $\nu$ ) および公開情報の ( $\varepsilon$ ,  $\nu$ )、チケット補助情報  $L$  は第3の対話プロトコルと同じである。ただし、 $L$  に含まれる  $i$  は、違すると通知を行うべき一定回数を意味している。第5の対話プロトコルの検証器3の手順を図17に従って説明し、証明器2の手順を図19に従って説明する。

【0118】 検証器3は、認証情報生成部286でチャレンジ  $C$  を生成して、認証情報保持部287に記録する(ステップ171)。検証しようとするチケットの識別子  $n$  と生成した  $C$  を、まとめて送信部281より証明器2へ送信する(ステップ172)。

【0119】 証明器2は、検証器3から送信された ( $C$ ,  $n$ ) を受信部292で受信して、情報保持部299に記録する(ステップ191)。チケット探索部122は受信した  $n$  に対応するチケットをチケット保持部121から探して、チケットを持っているかどうかを判定する(ステップ192)。対応するチケットを持たない場合には、レスポンス  $R$  に0を設定して、情報保持部299に記録する(ステップ197)。対応するチケットを持つ場合には、チケット  $t$ 、証明器2の手順  $Prover$ 、チケット付加情報  $L$  をセットする(ステップ193)。

【0120】 ステップ193が実行されたら、ステップ194を実行する。第5の対話プロトコルにおけるステップ194の詳細な手順を図25に示す。認証情報生成部296でチャレンジ  $x$  を生成して、第2の認証情報保持部298に記録する(ステップ251)。生成した  $x$  を送信部291から検証器3へ送信する(ステップ252)。

【0121】 検証器3は、 $x$  を受信部282で受信して、情報保持部289に記録する(ステップ173)。  $x$  として0を受信した場合は、証明器2がチケットを持っていないで、 $R$  として0を送ったことを意味するので、「無効」を意味する出力を出力部2812から出力して、対話プロトコルを終了する。第2の演算部284においてレスポンス  $\rho$  を、

【0122】

【数21】

$$\rho := x^{\delta} \bmod \nu$$

のように計算する(ステップ174)。計算した  $\rho$  を送信部281より証明器2へ送信する(ステップ17

5)。

【0123】 証明器2は、 $\rho$  を受信部292で受信して、情報保持部299に記録する(ステップ253)。第2の演算部294で

【0124】

【数22】

$$\rho := \rho^{\delta} \bmod \nu$$

を計算して、第2の認証情報保持部298に記録されている  $x$  と  $\rho$  が、一致するか判定する(ステップ254)。ステップ254の判定の結果が一致する場合には、内部状態保持部124の第2の内部状態保持部に確保されているカウンタ  $i$  の値をインクリメントする(ステップ255)。ステップ254の判定の結果が一致しない場合もしくはステップ255が実行されたら、内部状態保持部124に確保されている  $i$  の値と  $L$  より得られた上限値  $i$  とを比較する(ステップ256)。ステップ256の比較の結果として、 $i$  と  $i$  が等しくない場合は、第1の演算部293で  $R := C^n \bmod n$  を計算して、情報保持部299に記録する(ステップ257)。ステップ256の比較の結果として、 $i$  と  $i$  が等しい場合は、 $i$  を0に設定して(ステップ258)、第1の演算部293で

【0125】

【数23】

$$R := C^{D^2} \bmod n$$

を計算して、情報保持部299に記録する(ステップ2510)。ここまでの第5の対話プロトコルにおけるステップ194の詳細な手順である。

【0126】 ステップ194が実行されたら、ステップ193でセットされた  $t$ 、 $Prover$ 、 $L$  を解除する(ステップ195)。ステップ195もしくはステップ197が実行されたら、送信部291から検証器3へ  $R$  を送信する(ステップ196)。

【0127】 検証器3は、証明器2から送信された  $R$  を受信部282に受信して、情報保持部289に記録する(ステップ176)。  $R := R^{\delta} \bmod n$  を第1の演算部283で計算して情報保持部299に記録するとともに、この計算結果が、認証情報保持部287に記録されている  $C$  と一致するかを、正当性検証部285で判定する(ステップ177)。一致する場合は、0を出力部2812から出力する。一致しない場合は、 $R := R^{\delta} \bmod n$  を第1の演算部283でさらに計算して情報保持部299に記録するとともに、この計算結果が、認証情報保持部287に記録されている  $C$  と一致するかを、正当性検証部285で判定する(ステップ178)。ステップ178の結果が一致する場合は、証明器2のチケットが規定の度数に達したことを示すので、1を出力部2812から出力する。ステップ178の結果が一致しない場合は、「無効」を意味する出力を出力部

2 8 1 2 から出力する。

【 0 1 2 8 】以上が第 5 の対話プロトコルである。一定  
回数の利用があった場合に景品を授与するためのポイン

ト・カードとして、本プロトコルを適用できる。

【 0 1 2 9 】

【表 6】

#### 検証器

公開情報:  $(n, E)$

出力:  $M \in \{1(\text{有効}), 2(\text{レスポンス生成が一定の回数 } i \text{ に達した})\}$  もしくは '無効'

特権保証特徴情報:  $(\delta, \nu)$

```

C := rand
send (C, n)
receive  $\chi$ 
 $\rho := \chi^\delta \bmod \nu$ 
send  $\rho$ 
receive R
 $R := R^E \bmod n$ 
if  $C = R$ 
  output 1
else
   $R := R^E \bmod n$ 
  if  $C = R$ 
    output 2
  else
    output '無効'

```

#### Prover

```

 $\nu || \epsilon || i := L$ 
 $\chi := \text{rand}$ 
send  $\chi$ 
receive  $\rho$ 
 $\rho := \rho^\epsilon \bmod \nu$ 
if  $\rho = \chi$ 
   $i_n := i_n + 1$ 
else
  if  $i_n = i$ 
     $R := C^{D^2} \bmod n$ 
     $i_n := 0$ 
  else
     $R := C^D \bmod n$ 

```

【 0 1 3 0 】 【 2 . 8 . 第 6 の対話プロトコル】

(使い捨てのプリペイドカード型チケット、図 1 8、図 1 9、図 2 6) この発明における第 6 の対話プロトコルでは、特権を持つ検証者に対しては、チケットに係付けられた記憶領域中に保持される値を指定値だけ減少することができる。また、内部状態の更新がチケット発行時に定められた限界を越えるとそれを検証器 3 に通知する。

【 0 1 3 1 】一般的な検証者に対してもチケットの有効性の検証と記憶領域中に保持された値を伝達することができる。

【 0 1 3 2 】この対話プロトコルでは、検証器 3 から可変な指示情報が伝達され、証明器 2 からチケットに対応する可変な状態情報が伝達される。

【 0 1 3 3 】検証器 3 の特権を保証する特徴情報の

50  $(\delta, \nu)$  および公開情報の  $(\epsilon, \nu)$ 、チケット補助

情報 L は第 3 の対話プロトコルと同じである。ただし、L には特に i は含む必要がない。第 6 の対話プロトコルの検証器 3 の手順を図 18 に、証明器 2 の手順を図 19 にそれぞれ従って説明する。

【0134】検証器 3 は、認証情報生成部 286 でチャレンジ C を生成して、認証情報保持部 287 に記録する（ステップ 181）。検証しようとするチケットの識別子 n と生成した C を、まとめて送信部 281 より証明器 2 へ送信する（ステップ 182）。

【0135】証明器 2 は、検証器 3 から送信された (C, n) を受信部 292 で受信して、情報保持部 299 に記録する（ステップ 191）。チケット探索部 122 は受信した n に対応するチケットをチケット保持部 121 から探して、チケットを持っているかどうかを判定する（ステップ 192）。対応するチケットを持たない場合には、レスポンス R に 0 を設定して、情報保持部 299 に記録する（ステップ 197）。対応するチケットを持つ場合には、チケット t、証明器 2 の手順 Prover<sub>i</sub>、チケット付加情報 L をセットする（ステップ 193）。

【0136】ステップ 193 が実行されたら、ステップ 194 を実行する。第 6 の対話プロトコルにおけるステップ 194 の詳細な手順を図 26 に従って説明する。認証情報生成部 296 でチャレンジ x を生成して、第 2 の認証情報保持部 298 に記録する（ステップ 261）。生成した x を送信部 291 から検証器 3 へ送信する（ステップ 262）。

【0137】検証器 3 は、x を受信部 282 で受信して、情報保持部 289 に記録する（ステップ 183）。x として 0 を受信した場合は、証明器 2 がチケットを持っていないで、R として 0 を送ったことを意味するので、「無効」を意味する出力を出力部 2812 から出力して、対話プロトコルを終了する。入力部 2813 より入力されて入力情報保持部 2811 に予め記録されていたメッセージ μ を使って、第 2 の演算部 284 において

【0138】

【数 24】

$$\rho := (x || \mu)^e \bmod \nu$$

を計算する（ステップ 184）。計算したレスポンス ρ を送信部 281 より証明器 2 へ送信する（ステップ 185）。

【0139】証明器 2 は、ρ を受信部 292 で受信して、情報保持部 299 に記録する（ステップ 263）。第 2 の演算部 294 で

【0140】

【数 25】

$$\rho := \rho^d \bmod \nu$$

を計算して、情報保持部 299 に記録する（ステップ 264）。

64）。第 2 の認証情報保持部 298 に記録されている x と計算した ρ の上位の桁とが、一致するか判定する（ステップ 265）。ステップ 265 の判定の結果が一致しない場合には、内部状態保持部 124 の内部状態保持部に確保されているカウンタ i<sub>1</sub> の値を利用して、メッセージとして M := 1 || i<sub>1</sub> を設定して、情報保持部 299 に記録する（ステップ 2613）。ステップ 265 の判定の結果が一致する場合には、ρ の下位の桁から μ を取り出して、i<sub>1</sub> の値を i<sub>1</sub> := i<sub>1</sub> - μ のように減算する（ステップ 265）。M := 0 || i<sub>1</sub> を設定して、情報保持部 299 に記録する（ステップ 267）。i<sub>1</sub> が 0 より小さいか判定する（ステップ 268）。0 より小さい場合には、内部状態保持部 124 から i<sub>1</sub> を解放して（ステップ 2611）、チケット保持部 121 から t を削除する（ステップ 2612）。いずれの場合でも、第 1 の演算部 293 で R := (C || M)<sup>d</sup> mod n を計算して、情報保持部 299 に記録する（ステップ 269）。ここまでする第 6 の対話プロトコルにおけるステップ 194 の詳細な手順である。

【0141】ステップ 194 が実行されたら、ステップ 193 でセットされた t、Prover<sub>i</sub>、L を解除する（ステップ 195）。ステップ 195 もしくはステップ 197 が実行されたら、送信部 291 から検証器 3 へ R を送信する（ステップ 196）。

【0142】検証器 3 は、証明器 2 から送信された R を受信部 282 に受信して、情報保持部 289 に記録する（ステップ 186）。R := R<sup>e</sup> mod n を第 1 の演算部 283 で計算して情報保持部 299 に記録する（ステップ 187）。この計算結果の上位の桁が、認証情報保持部 287 に記録されている C と一致するかを、正当性検証部 285 で判定する（ステップ 188）。一致する場合は、R の下位の桁から M を取り出して（ステップ 189）、出力部 2812 から出力する。一致しない場合は、「無効」を意味する出力を出力部 2812 から出力する。

【0143】以上が第 6 の対話プロトコルである。検証器 3 の出力が「無効」以外の値の時は、出力の最上位のビットによってカウンタの減算の実行の有無を確認できて、その下の桁でカウンタ i<sub>1</sub> の値を確認できる。特権のない検証器 3 でも、レスポンス ρ に適当な値（例えば 1）を送ることで、カウンタの値を変更せずに、カウンタの値を調べられる。例えば、チケットを初期化する時にカウンタ i<sub>1</sub> を決められた値に設定して、サービスを利用する度に、対価をカウンタから減算するように本プロトコルを適用することで、プリペイドカードの機能を提供できる。

【0144】

【表 7】

**検証器**公開情報:  $(n, E)$ 入力:  $\mu$  (減少度数)出力:  $M$  もしくは '無効'特権保証特徴情報:  $(\delta, \nu)$ 

```

C := rand
send (C, n)
receive  $\chi$ 
 $\rho := (\chi || \mu)^\delta \bmod \nu$ 
send  $\rho$ 
receive R
 $R := R^E \bmod n$ 
if  $R = C || M$ 
    output M
else
    output '無効'

```

**Prover**

```

 $\chi := rand$ 
send  $\chi$ 
receive  $\rho$ 
 $\rho := \rho^\delta \bmod \nu$ 

if  $\rho = \chi || \mu$ 
     $i_n := i_n - \mu$ 
     $M := 0 || i_n$ 
    if  $i_n < 0$ 
        free  $i_n$ 
    delete t
else
     $M := 1 || i_n$ 
 $R := (C || M)^D \bmod n$ 

```

【0145】 [2. 9. 第7の対話プロトコル]

(再充填可能なブリペイドカード型のチケット、図18、図19、図27) この発明における第7の対話プロトコルは、第6の対話プロトコルの変形であって、特権を持つ検証者に対しては、チケットに関係付けられた記憶領域中に保持された値を指定して増減することができる。

【0146】 第6の対話プロトコルと同様に、一般的な検証者に対してもチケットの有効性に対応する内部状態を検証することができる。

【0147】 この対話プロトコルでは、検証器3から可変な指示情報が伝達され、証明器2からもチケットに対応する可変な状態情報が伝達される。

【0148】 検証器3の特権を保証する特徴情報の

$(\delta, \nu)$  および公開情報の  $(E, \nu)$ 、チケット補助

情報Lは第6の対話プロトコルと同じである。第7の対話プロトコルの検証器3の手順を図18に、証明器2の手順を図19にそれぞれ従って説明する。

【0149】 検証器3は、認証情報生成部286でチャレンジCを生成して、認証情報保持部287に記録する(ステップ181)。検証しようとするチケットの識別子nと生成したCを、まとめて送信部281より証明器2へ送信する(ステップ182)。

【0150】 証明器2は、検証器3から送信された  $(C, n)$  を受信部292で受信して、情報保持部299に記録する(ステップ191)。チケット探索部122は受信したnに対応するチケットをチケット保持部121から探して、チケットを持っているかどうかを判定する(ステップ192)。対応するチケットを持たない場合には、レスポンスRに0を設定して、情報保持部2

99に記録する(ステップ197)。対応するチケットを持つ場合には、チケット $t$ 、証明器2の手順 $Prover$ 、チケット付加情報 $L$ をセットする(ステップ193)。

【0151】ステップ193が実行されたら、ステップ194を実行する。第7の対話プロトコルにおけるステップ194の詳細な手順を図27に従って説明する。認証情報生成部296でチャレンジ $x$ を生成して、第2の認証情報保持部298に記録する(ステップ271)。生成した $x$ を送信部291から検証器3へ送信する(ス

テップ272)。  
【0152】検証器3は、 $x$ を受信部282で受信して、情報保持部289に記録する(ステップ183)。 $x$ として0を受信した場合は、証明器2がチケットを持っていないで、 $R$ として0を送ったことを意味するので、「無効」を意味する出力を出力部2812から出力して、対話プロトコルを終了する。入力部2813より入力されて入力情報保持部2811に予め記録されていたメッセージ $\mu$ を使って、第2の演算部284において

【0153】

【数26】

$$\rho := (x || \mu)^s \bmod \nu$$

を計算する(ステップ184)。計算したレスポンス $\rho$ を送信部281より証明器2へ送信する(ステップ185)。

【0154】証明器2は、 $\rho$ を受信部292で受信して、情報保持部299に記録する(ステップ273)。第2の演算部294で

【0155】

【数27】

$$\rho := \rho^t \bmod \nu$$

を計算して、情報保持部299に記録する(ステップ274)。第2の認証情報保持部298に記録されている $x$ と計算した $\rho$ の上位の桁とが、一致するか判定する(ステップ275)。ステップ275の判定の結果が一

致しない場合には、内部状態保持部124の第2の内部状態保持部に確保されているカウンタ $i$ の値を利用して、メッセージとして $M := 1 || i$ を設定して、情報保持部299に記録する(ステップ2712)。ステップ275の判定の結果が一致する場合には、 $\rho$ の下位の桁から $\mu$ を取り出して、 $i$ の値を $i := i - \mu$ のように減算する(ステップ275)。 $M := 0 || i$ を設定して、情報保持部299に記録する(ステップ277)。 $i$ が0より小さいか判定する(ステップ278)。0より小さい場合には、 $i$ を0に設定する(ステップ2711)。いずれの場合でも、第1の演算部293で $R := (C || M)^s \bmod n$ を計算して、情報保持部299に記録する(ステップ279)。ここまですべて第7の対話プロトコルにおけるステップ194の詳細な手順である。

【0156】ステップ194が実行されたら、ステップ193でセットされた $t$ 、 $Prover$ 、 $L$ を解除する(ステップ195)。ステップ195もしくはステップ197が実行されたら、送信部291から検証器3へ

20  $R$ を送信する(ステップ196)。

【0157】検証器3は、証明器2から送信された $R$ を受信部282に受信して、情報保持部289に記録する(ステップ186)。 $R := R^t \bmod n$ を第1の演算部283で計算して情報保持部299に記録する(ステップ187)。この計算結果の上位の桁が、認証情報保持部287に記録されている $C$ と一致するかを、正当性検証部285で判定する(ステップ188)。一致する場合は、 $R$ の下位の桁から $M$ を取り出して(ステップ189)、出力部2812から出力する。一致しない場合は、「無効」を意味する出力を出力部2812から出力する。

【0158】以上が第7の対話プロトコルである。

【0159】

【表8】



43

**検証器**公開情報:  $(n, E)$ 入力:  $\mu$ 出力:  $M$  もしくは '無効'特権保証特徴情報:  $(\delta, \nu)$ 

```

C := rand
send (C, n)
receive  $\chi$ 
 $\rho := (\chi || \mu)^\delta \bmod \nu$ 
send  $\rho$ 
receive R
 $R := R^E \bmod n$ 
if  $R = C || M$ 
    output M
else
    output '無効'

```

```

Prover
 $\nu || \varepsilon := L$ 
 $\chi := \text{rand}$ 
send  $\chi$ 
receive  $\rho$ 
 $\rho := \rho^\varepsilon \bmod \nu$ 
if  $\rho = \chi || \mu$ 
     $i_n := i_n - \mu$ 
     $M := 0 || i_n$ 
    if  $i_n < 0$ 
         $i_n := 0$ 
else

```

```

     $M := 1 || i_n$ 
 $R := (C || M)^D \bmod n$ 

```

【0160】 [2. 10. 第8の対話プロトコル]

(回数券型チケットー無効化・払い戻し処理、図16、図19、図24) この発明における第8の対話プロトコルでは、チケットに対して有効か無効かを表すフラグが証明器2の内部状態として対応し、特権のある検証者が40 チケットを無効化することが可能である。

【0161】 検証器3の特権を保証する特徴情報の  $(\delta, \nu)$  および公開情報の  $(\varepsilon, \nu)$ 、チケット補助情報Lは第3の対話プロトコルと同じである。第8の対話プロトコルの検証器3の手順を図16に、証明器2の手順を図19にそれぞれ従って説明する。ただし、対話プロトコルに先立って、検証を実行するのか、チケットの無効化を実行するのかを、検証器3の入力部2813より入力されて、入力情報保持部2811に記録されているとする。

44

【0162】 検証器3は、認証情報生成部286でチャレンジCを生成して、認証情報保持部287に記録する(ステップ161)。検証しようとするチケットの識別子nと生成したCを、まとめて送信部281より証明器2へ送信する(ステップ162)。

【0163】 証明器2は、検証器3から送信された  $(C, n)$  を受信部292で受信して、情報保持部299に記録する(ステップ191)。チケット探索部122は受信したnに対応するチケットをチケット保持部121から探して、チケットを持っているかどうかを判定する(ステップ192)。対応するチケットを持たない場合には、レスポンスRに0を設定して、情報保持部299に記録する(ステップ197)。対応するチケットを持つ場合には、チケットt、証明器2の手順Prover、チケット付加情報Lをセットする(ステップ1

93)。

【0164】ステップ193が実行されたら、ステップ194を実行する。第8の対話プロトコルにおけるステップ194の詳細な手順を図24に従って説明する。認証情報生成部296でチャレンジ $x$ を生成して、第2の認証情報保持部298に記録する(ステップ241)。生成した $x$ を送信部291から検証器3へ送信する(ステップ242)。

【0165】検証器3は、 $x$ を受信部282で受信して、情報保持部289に記録する(ステップ163)。 $x$ として0を受信した場合は、証明器2がチケットを持っていないで、 $R$ として0を送ったことを意味するので、「無効」を意味する出力を出力部2812から出力して、対話プロトコルを終了する。あらかじめ、通常の検証を行う場合には $\mu := 1$ として、チケットを無効化する場合には $\mu := 2$ として、 $\mu$ の値を入力部2813より与えて入力情報保持部2811に記録しておき、第2の演算部284において、

【0166】

【数28】

$$\rho := x^{\mu} \bmod \nu$$

としてレスポンス $\rho$ を計算する(ステップ164)。計算した $\rho$ を送信部281より証明器2へ送信する(ステップ165)。

【0167】証明器2は、 $\rho$ を受信部292で受信して、情報保持部299に記録する(ステップ243)。第2の演算部294で

【0168】

【数29】

$$\rho := \rho^{\mu} \bmod \nu$$

を計算して、第2の認証情報保持部298に記録されている $x$ と $\rho$ が、一致するか判定する(ステップ244)。ステップ244の判定の結果が一致する場合にはステップ245の代わりに、 $M$ に0を設定して情報保持部299に記録する。ステップ244の判定の結果が一致しない場合には、第2の演算部294で

【0169】

【数30】

$$\rho := \rho^{\mu} \bmod \nu$$

を計算して、第2の認証情報保持部298に記録されている $x$ と $\rho$ が、一致するか判定する(ステップ248)。ステップ248の判定の結果が一致する場合にはステップ249の代わりに、内部状態保持部124の第2の内部状態保持部に確保されているカウンタ $i$ の値を0以外の値(例えば1)に設定する。ステップ248の判定の結果が一致しない場合には、メッセージ $M$ に1を設定して、情報保持部299に記録する(ステップ2411)。いずれの場合においても次にステップ247の代わりに、 $i$ の値が0であるか確認する。 $i$ の値が0の場合は、第1の演算部293で $R := (C || M)$

$\rho \bmod n$ を計算して、情報保持部299に記録する(ステップ248)。 $i$ が0でない場合は、 $R$ の値を1に設定して情報保持部299に記録する(ステップ2410)。ここまでの第8の対話プロトコルにおけるステップ194の詳細な手順である。

【0170】ステップ194が実行されたら、ステップ193でセットされた $t$ 、 $Prover$ 、 $L$ を解除する(ステップ195)。ステップ195もしくはステップ197が実行されたら、送信部291から検証器3へ $R$ を送信する(ステップ196)。

【0171】検証器3は、証明器2から送信された $R$ を受信部282に受信して、情報保持部289に記録する(ステップ166)。 $R := R^{\mu} \bmod n$ を第1の演算部283で計算する(ステップ167)。この計算結果の上位の桁が、認証情報保持部287に記録されている $C$ と一致するかを、正当性検証部285で判定する(ステップ168)。一致する場合は証明器2が有効なチケットを持っていることが示されたので、 $R$ の下位の桁より取り出した $M$ を、証明器2から受け取った情報として取り出して(ステップ169)、出力部2812から出力する。一致しない場合は、現対話で無効にした場合も含めて、証明器2が有効なチケットを持つことが示されなかったので、「無効」を意味する出力を出力部2812から出力する。

【0172】以上が第8の対話プロトコルである。カウンタ $i$ の値が1に設定されると、 $D$ を利用したレスポンスを送信できなくなるので、チケットの無効化となる。一度利用したら無効になるチケットや、チケットの払い戻しなどでチケットを無効にする必要がある場合に、本プロトコルが適用できる。

【0173】

【表9】

## 検証器

公開情報:  $(n, E)$ 入力:  $\mu$  (1: 通常, 2: チケットの無効化)出力:  $M$  もしくは '無効'特権保証特徴情報:  $(\nu, \delta)$  $C := \text{rand}$  $\text{send } (C, n)$  $\text{receive } x$  $\rho := x^{\delta} \bmod \nu$  $\text{send } \rho$  $\text{receive } R$  $R := R^E \bmod n$  $\text{if } R = C || M$  $\text{output } M$  $\text{else}$  $\text{output '無効'}$ 

Prover

 $\nu || \varepsilon := L$  $x := \text{rand}$  $\text{send } x$  $\text{receive } \rho$  $\rho := \rho^{\varepsilon} \bmod \nu$  $\text{if } \rho = x$  $M := 0$  $\text{else}$  $\rho := \rho^{\varepsilon} \bmod \nu$  $\text{if } \rho = x$  $i_n := 1$  $\text{else}$  $M := 1$  $\text{if } i_n = 0$  $R := (C || M)^D \bmod n$  $\text{else}$  $R := 1$  $\text{free } i_n$ 

【0174】【2.11. 第9の対話プロトコル】

(チケット利用の証拠の生成、図18) この発明における第9の対話プロトコルでは、特権を有する検証者は、証明器2に対して行なった検証の証拠を残すことができる。

【0175】本対話プロトコルでは検証器3の認証情報生成部が $r$ を保持し、また一方向性関数 $H$ を施すことによりチャレンジ $C$ を生成することと、 $(r, R)$ を利用証拠情報保持部に蓄積することが特徴であり、証明器側の手順には依存しない。したがって、すでに述べた第

1ないし第8のプロトコル全てに適用できる。

【0176】検証器3の特権を保証する特徴情報の $(\delta, \nu)$ は、第6の対話プロトコルと同じである。第9の対話プロトコルを、図18の検証器3の手順に適用した例を示す。ただし、対話プロトコルに先立って、検証器3から証明器2へ伝えるメッセージ $\mu$ が、検証器3の入力部2813より入力されて、入力情報保持部2811に記録されているとする。

【0177】認証情報生成部286において、乱数 $r$ を生成し、それを $C := H(r)$ のように一方向性関数に通してチャレンジ $C$ を生成し、認証情報保持部287に記録する(ステップ181)。検証しようとするチケットの識別子 $n$ と生成した $C$ を、まとめて送信部281より証明器2へ送信する(ステップ182)。

【0178】証明器2から送られてきた $x$ を、受信部282で受信して、情報保持部289に記録する(ステップ183)。 $x$ として0を受信した場合は、証明器2がチケットを持っていないで、 $R$ として0を送ったことを意味するので、「無効」を意味する出力を出力部2812から出力して、対話プロトコルを終了する。第2の演算部284においてレスポンス $\rho$ を、

【0179】

【数31】

$$\rho := (x || \mu)^{\delta} \bmod \nu$$

のように計算する(ステップ184)。計算した $\rho$ を送信部281より証明器2へ送信する(ステップ185)。

【0180】証明器2から送信されたレスポンス $R$ を受信部282で受信して、情報保持部289に記録する(ステップ186)。 $R^{\varepsilon} \bmod n$ を第1の演算部283で計算する(ステップ187)。この計算結果の上位の桁が、認証情報保持部287に記録されている $C$ と一致するかを、正当性検証部285で判定する(ステップ188)。ステップ188で一致した場合は、ステップ181で生成した乱数 $r$ と、ステップ186で情報保持部289に記録した $R$ とを組にして、利用証拠情報保持部2814に記録する。さらに、 $R$ の下位の桁より取り出した $M$ を、証明器2から受け取った情報として取り出して(ステップ189)、出力部2812から出力する。ステップ188で一致しなかった場合は、「無効」を意味する出力を出力部2812から出力する。

【0181】以上が第9の対話プロトコルを、図18の検証器3の手順に適用した例である。

【0182】商品券や宝くじのように、利用者と代理人(加盟店)がチケットの対価交換を済ませ、代理人がチケットの管理者に対価交換済みのチケットを送付ないしは報告するという形態のチケットの実現を想定する。チケット検証がチケットの譲渡に相当するので、その証拠を残すことができれば、代理人とチケットの管理者との間に強い信頼関係を仮定せずにチケットの譲渡が実現で

きる。

【0183】利用証拠情報保持部2814に記録される情報は、本実施例のように、検証器3と証明器2のあいだで通信された情報であってもよいし、それらの情報の一部であってもよい。まら、その情報に一方方向性ハッシュ

公開情報:  $(n, E)$

検証器を特権化する情報:  $(\nu, \delta)$

入力:  $\mu$

出力:  $M$  または  $invalid$

検証器

$r := rand$

$C := H(r)$

send  $(C, n)$

receive  $\chi$

$\rho := (\chi || \mu)^\delta \bmod \nu$

send  $\rho$

receive  $R$

if  $R^E \bmod n = C || M$

output  $M$

store  $(r, R)$

else

output  $invalid$

【0185】【2.12.第10の対話プロトコル】

(センター管理型のプリペイドカード型チケット、図18、図19、図27)この発明における第10の対話プロトコルでは、証明器2はセンターが操作可能な度数保持手段を持ち、第9の検証プロトコルにおける、特権を有する検証者とのチケット検証に伴い度数を減じ、減じた度数情報の証拠が検証器3に保持される。

【0186】検証器3の検証手順は第9のプロトコルと同じである。以下は証明器2のプロトコルを説明する。

【0187】検証器3の特権を保証する特徴情報の $(\delta, \nu)$ および公開情報の $(\varepsilon, n)$ 、チケット補助情報 $L$ は第6の対話プロトコルと同じである。第10の対話プロトコルの検証器3の手順は第9の対話プロトコルと同じである。検証器3の手順を図18に、証明器2の手順を図19にそれぞれ従って説明する。

【0188】認証情報生成部286において、乱数 $r$ を生成しそれを一方方向性関数に通してチャレンジ $C$ を生成し、認証情報保持部287に記録する(ステップ181)。検証しようとするチケットの識別子 $n$ と生成した $C$ を、まとめて送信部281より証明器2へ送信する(ステップ182)。

【0189】証明器2は、検証器3から送信された $(C, n)$ を受信部292で受信して、情報保持部299に記録する(ステップ191)。チケット探索部122は受信した $n$ に対応するチケットをチケット保持部1

ユ関数などの所定の演算を施したものの、あるいは上記のもの組み合わせであってもよい。

【0184】

【表10】

21から探して、チケットを持っているかどうかを判定する(ステップ192)。対応するチケットを持たない場合には、レスポンス $R$ に0を設定して、情報保持部299に記録する(ステップ197)。対応するチケットを持つ場合には、チケット $t$ 、証明器2の手順 $Prover$ 、チケット付加情報 $L$ をセットする(ステップ193)。

【0190】ステップ193が実行されたら、ステップ194を実行する。第10の対話プロトコルにおけるステップ194の詳細な手順は図27の変形である。認証情報生成部296でチャレンジ $\chi$ を生成して、第2の認証情報保持部298に記録する(ステップ271)。生成した $\chi$ を送信部291から検証器3へ送信する(ステップ272)。

【0191】検証器3は、 $\chi$ を受信部282で受信して、情報保持部289に記録する(ステップ183)。 $\chi$ として0を受信した場合は、証明器2がチケットを持っていないで、 $R$ として0を送ったことを意味するので、「無効」を意味する出力を出力部2812から出力して、対話プロトコルを終了する。入力部2813より入力されて入力情報保持部2811に予め記録されていたメッセージ $\mu$ を使って、第2の演算部284において

【0192】

【数32】

$$\rho := (\chi || \mu)^\delta \bmod \nu$$

を計算する(ステップ184)。計算したレスポンス $\rho$ を送信部281より証明器2へ送信する(ステップ185)。

【0193】証明器2は、 $\rho$ を受信部292で受信して、情報保持部299に記録する(ステップ273)。

第2の演算部294で

【0194】

【数33】

$$\rho := \rho' \bmod \nu$$

を計算して、情報保持部299に記録する(ステップ274)。第2の認証情報保持部298に記録されている $x$ と計算した $\rho$ の上位の桁とが、一致するか判定する(ステップ275)。

ステップ275の判定の結果が一致しない場合には、メッセージとして $M := 1 || i$ を設定して、情報保持部299に記録する(ステップ2712)。ステップ275の判定の結果が一致する場合には、ステップ276とステップ277の代わりに、 $\rho$ の下位の桁から $\mu$ を取り出して、入力情報保持部2911に記録して、 $M$ に0を設定して、情報保持部299に記録する。ステップ278の代わりとして、内部状態保持部124の第1の内部状態保持部に記録されている $j$ が、取り出した $\mu$ 以上であるか判定する。 $j$ が $\mu$ 以上である場合には、ステップ2711の代わりに、 $j := j - \mu$ として $j$ の値を変更して、 $M := M || \mu$ として $M$ の値を変更する。 $j$ が $\mu$ より小さい場合には、 $j$ の値を0に変更して、 $M := M || j$ として $M$ の値を変更する。いずれの場合でも、第1の演算部293で $R := (C || M)^{\rho} \bmod n$ を計算して、情報保持部299に記録する(ステップ2710)。ここまでの第10の対話プロトコルにおけるステップ194の詳細な手順である。

【0195】ステップ194が実行されたら、ステップ193でセットされた $t$ 、 $Prover$ 、 $L$ を解除す

る(ステップ195)。ステップ195もしくはステップ197が実行されたら、送信部291から検証器3へ $R$ を送信する(ステップ196)。

【0196】検証器3は、証明器2から送信されたレスポンス $R$ を受信部282に受信して、情報保持部289に記録する(ステップ186)。 $R^{\rho} \bmod n$ を第1の演算部283で計算する(ステップ187)。この計算結果の上位の桁が、認証情報保持部287に記録されている $C$ と一致するかを、正当性検証部285で判定する(ステップ188)。ステップ188で一致した場合は、ステップ181で生成した乱数 $r$ と、ステップ186で情報保持部289に記録した $R$ とを組にして、利用証情報保持部2814に記録する。さらに、 $R$ の下位の桁より取り出した $M$ を、証明器2から受け取った情報として取り出して(ステップ189)、出力部2812から出力する。ステップ188で一致しなかった場合は、「無効」を意味する出力を出力部2812から出力する。

【0197】以上が第10の対話プロトコルである。第7の対話プロトコルでは、チケット毎に独立のカウンタ1からメッセージ $\mu$ の値だけ減算していた。本プロトコルは、チケットとは独立の内部状態を減算しているところが異なる。第7のプロトコルは、チケット一つが独立のプリペイドカードに適用できるのに対して、本プロトコルは、共通のプリペイドカードによって、複数のチケットから構成されるサービスを提供できる。例えば、施設内で飲食と娯楽は別のチケットの団体が提供して、利用するときにはそれぞれ別のチケットを必要とするが、それぞれの利用に応じて、あらかじめ購入した一つのプリペイドカードから対価を減じることができる。

【0198】

【表11】

53  
**Prover**  
 $f||\nu||\epsilon := L$   
**if**  $f$   
      $\chi := \text{rand}$   
     **send**  $\chi$   
     **receive**  $\rho$   
     **if**  $\rho^\epsilon \bmod \nu = \chi||\mu$   
          $M := 0$   
         **if**  $\mu \leq j$   
              $j := j - \mu$   
              $M := M||\mu$   
         **else**  
              $M := M||j$   
              $j := 0$   
     **else**  
          $M := 1||j$   
 $R := (C||M)^\rho \bmod n$

54

【0199】【2.13. 第11の対話プロトコル】  
 (複数の対話プロトコルを実装) この発明における第11の対話プロトコルでは、証明器2は予め決められた複数の証明手順を行なえる。証明器2には複数の証明手順を実行可能な証明手順実行部があり、予め決められた証明手順のいずれかを選択して実行する。手順の選択はチケット付加情報Lの一部を用いて行なえる。

【0200】【2.14. 第12の対話プロトコル】  
 (チケット付加情報を用いた証明手順の付与、図19、図31) この発明における第12の対話プロトコルでは、証明器2に証明手順を与えることができる。

【0201】証明器2に制御手段があり、Lに証明手順の一部を与えることによって証明手順を与えることができる。

【0202】証明手順の与えかたは、手順を記述する記述言語を利用して完全に自由な記述を許す方法も可能である。しかし、ある程度の汎用性のある固定の手順を用意しておき、その各ブロックの手順を記述言語でLに記述してもよい。後者の方法は、比較的小さい情報量で表現できる利点を持っている。

【0203】第12の対話プロトコルの証明器2の手順を図19および図31に従って説明する。Lの中に、検証器3の検証の実行の有無  $f$ 、検証器3の検証に必要な公開情報  $(\nu, \epsilon)$ 、証明手順の命令群  $P_i$  が含まれている。また、命令群  $P_i$  には、何もしないという命令も記述できるとする。例えば、Lが  $(f, \nu, \epsilon, P_1, P_1, P_1, P_1, P_1, P_1)$  のように構成されているとする。

【0204】受信部292で検証器3から  $(C, n)$  を受信して(ステップ191)、情報保持部299に記録する。チケット探索部122は受信した  $n$  に対応するチ

20 ケットをチケット保持部121から探して、チケットを持っているかどうかを判定する(ステップ192)。対応するチケットを持たない場合には、レスポンス  $R$  に0を設定して、情報保持部299に記録する(ステップ197)。対応するチケットを持つ場合には、チケット  $t$ 、証明器2の手順  $P_{\text{Prover}_i}$ 、チケット付加情報  $L$  をセットする(ステップ193)。第12の対話プロトコルでは、 $P_{\text{Prover}_i}$  のセットにおいて、 $L$  から  $(f, \nu, \epsilon, P_1, P_1, P_1, P_1, P_1, P_1)$  を取り出して記録する。

30 【0205】ステップ193が実行されたら、ステップ194を実行する。第1の対話プロトコルにおけるステップ194の詳細な手順を図31に示す。 $f$  が真であるか判定する(ステップ3101)。 $f$  が正しければ、ステップ3102からステップ3109までを実行する。

【0206】認証情報生成部296で乱数  $x$  を生成して、第2の認証情報保持部298に記録する(ステップ3102)。送信部291より検証部2へ  $x$  を送信する(ステップ3103)。検証部2から送信された  $\rho$  を受信部292で受信して、情報保持部299に記録する

40 (ステップ3104)。

【0207】

【数34】

$$\rho^\epsilon \bmod \nu$$

を計算して上位の桁が、 $x$  と等しいか比較する(ステップ3105)。ステップ3105の結果が等しい場合には、ステップ3106とステップ3107を実行する。 $M$  に0を設定して情報記録部299に記録する(ステップ3106)。 $P_i$  の命令もしくは命令群を実行する(ステップ3107)。ステップ3105の結果が等しくない場合には、ステップ3108とステップ3109

を実行する。Mに1を設定して情報記録部299に記録する(ステップ3108)。P<sub>i</sub>の命令もしくは命令群を実行する(ステップ3109)。

【0208】P<sub>i</sub>の命令もしくは命令群を実行する(ステップ3110)。P<sub>i</sub>の命令もしくは命令群を実行して、結果が真であるか判定する(ステップ3111)。ステップ3111の結果が真の場合は、ステップ3112とステップ3113を実行する。P<sub>i</sub>の命令もしくは命令群を実行する(ステップ3112)。R := (C | M)<sup>0</sup> mod nを第1の演算部293で計算し、情報保持部299に記録する(ステップ3113)。ステップ3111の結果が真でない場合には、ステップ3114とステップ3115を実行する。P<sub>i</sub>の

命令もしくは命令群を実行する(ステップ3114)。Rを1に設定して、情報保持部299に記録する(ステップ3115)。ここまでの第1の対話プロトコルにおけるステップ194の詳細な手順である。

【0209】ステップ194が実行されたら、ステップ193でセットされたt、Prover<sub>i</sub>、Lを解除する(ステップ195)。ステップ195もしくはステップ197が実行されたら、送信部291から検証器3へRを送信する(ステップ196)。

【0210】以上が第12の対話プロトコルにおける証明器2の手順である。

【0211】

【表12】

57

公開情報:  $(n, E)$ 検証器を特権化する情報:  $(\nu, \delta)$ 入力:  $\mu$ 出力:  $M$  または **invalid****検証器** $C := \text{rand}$ **send**  $(C, n)$ **receive**  $\chi$  $\rho := (\chi || \mu)^\delta \bmod \nu$ **send**  $\rho$ **receive**  $R$ **if**  $R^E \bmod n = C || M$     **output**  $M$ **else**    **output** **invalid****証明器****receive**  $(C, n)$ **find**  $(n, t, L)$  $f || \nu || e || P_0 || P_1 || P_2 || P_3 || P_4 || P_5 := L$ **if**  $f$      $\chi := \text{rand}$     **send**  $\chi$     **receive**  $\rho$     **if**  $\rho^e \bmod \nu = \chi || \mu$          $M := 0$          $P_0$     **else**         $M := 1$          $P_1$          $P_2$     **if**  $P_3$          $P_4$          $R := (C || M)^D \bmod n$     **else**         $P_5$          $R := \text{undefind}$     **send**  $R$ 

【0212】 [2. 15. 第13の対話プロトコル]

(検証器3の構成、図30) この発明における第13の検証プロトコルでは、検証器3の特権を与える特徴情報をチケットとして与え、検証器3の特権保証特徴情報による符号化は前述までのチケット証明器2と同様に与える。

【0213】 図30はこの検証プロトコルを行なう検証器3の構成図である。

【0214】 検証器3は特権を保証する秘密情報 $\delta$ による符号化を行なう場合、チケット保持部114から対応するチケットを取りだし、固有情報保持部113に保持

40 された固有情報を基に符号化する。

【0215】 [3. 第2の実施例]

【3. 1. 認証手法】 本実施例では、チケットの特徴情報は、以下の形で与えられる。

【0216】  $p$ は素数であり、 $G$ は離散対数問題が困難な有限群であり、 $g$ は有限群 $G$ の位数 $p$ の元であり、 $y = g^x$ が満たされるとき、 $(p, G, g, y, x)$ がチケットの特徴情報である。特に、 $(p, G, g, y)$ を公開の特徴情報とし、 $x$ を秘密の特徴情報とする場合について、実現できるチケットの証明方法について詳述する。



【0217】実際には、 $G$ を有限体の乗法群として構成したり、有限体上の楕円曲線として構成することができる。

【0218】例えば、 $(p, G, g)$ をシステム共通とし、公開情報 $y$ 、秘密情報 $x$ とする。チケットはチケット特徴情報 $x$ と証明器固有情報 $d_i$ とチケット付加情報 $L$ より計算されるデータであり、証明器2が $(C, y, t, L)$ に対して証明器固有情報 $d_i$ を用いて $\tau(C, y, t, L) = C'$ が計算できるように構成する。

【0219】例えば、 $d_i$ をある暗号系の復号鍵とし、 $E_i$ を $d_i$ に対応する暗号化とし、 $H$ を一方向性関数としたとき、 $t := (E_i(x), H(d_i || x || L))$ のように定めることができる。

【0220】チケットを上述の様に定義すると、チケットを用いた秘密の特徴情報 $x$ による符号化 $C'$ は、入力 $(C, y, t, L)$ に対して証明器2の固有情報 $d_i$ によって $E_i(D)$ を復号して証明器2中で $D$ を回復し、その値を用いて一方向性関数の値をチケットと比較することによって $L$ の値の正当性を確認し、回復された $D$ の値を用いて証明器2内で $C'$ を計算するようにすれば良い。

【0221】また、 $d_i$ を一方向性関数として、 $t = x - d_i(L, y)$ と定めることもできる。

【0222】チケットの上述の定義によれば、入力 $(C, y, t, L)$ に対して $D$ による符号化は $C' = C' \oplus d_i(L, y)$ を計算することによって行なうこともできる。

【0223】まずは離散対数問題の困難さに安全性の根拠をおく、秘密値共有の原理を利用した対話プロトコルの例を挙げる。

【0224】〔3.2.第14の対話プロトコル〕  
(証明器2が時計を持つ定期券型のチケット、図13、図19、図20)第14の対話プロトコルでは、証明器2の内部状態として時計情報を持っているとする。本プロトコルにおける検証器3の手順を図13に、証明器2の手順を図19に従って説明する。

【0225】検証器3は、認証情報生成部286によって乱数 $r$ を生成して、 $C := g^r$ としてチャレンジ $C$ を生成して、認証情報保持部287に記録する(ステップ131)。ステップ132の代わりに、認証情報保持部287に記録された $C$ と、公開情報 $y$ をまとめて、送信部281より証明器2へ送信する。

【0226】ステップ191の代わりに、証明器2は、検証器3から送信された $(C, y)$ を受信部292で受信して、情報保持部299に記録する。チケット探索部122は受信した $y$ に対応するチケットをチケット保持部121から探して、チケットを持っているかどうかを判定する(ステップ192)。レスポンス $R$ にチケットを持たないことを意味する値(この場合は0)を設定して、情報保持部299に記録する(ステップ197)。

ステップ192の判定の結果として対応するチケットを持つ場合には、チケット $t$ 、証明器2の手順 $Prover$ 、チケット付加情報 $L$ を制御部2912内にセットする(ステップ193)。

【0227】ステップ193が実行されたら、ステップ194を実行する。この対話の例におけるステップ194の詳細な手順を図20に従って説明する。内部状態保持部124の第2の内部状態保持部から読み出したその時の時刻 $time$ と、 $L$ に記述されている有効期限とを比較して、チケットがその時点で有効であるか判定する(ステップ201)。チケットを有効であると判定した場合には、第1の演算部293において $R$ を、 $R := C'$ のように計算して、情報保持部299に記録する(ステップ202)。特に $R$ のこの計算を、証明器2の中の第1の演算部293ですべて計算してもよいが、チケット $t$ が $t = x - d_i(L, y)$ のように構成されている場合には、 $C'$ の計算は $C' = C' \oplus d_i(L, y)$ のようにも計算できるので、 $C'$ を証明器2の外で計算して、証明器2の中の第1の演算部293で計算した $C' \oplus d_i(L, y)$ とを証明器2の外で掛け合わせても計算できる。証明器2の計算速度が遅い場合には、このような方法も有効になる。ステップ201においてチケットを無効であると判定した場合には、必要であるならばチケットをチケット保持部121から削除して(ステップ203)、 $R$ に1を設定して、情報保持部299に記録する(ステップ204)。ここまでがこの対話の例におけるステップ194の詳細な手順である。

【0228】ステップ194が実行されたら、ステップ193でセットされた $t$ 、 $Prover$ 、 $L$ を制御部2912から解除する(ステップ195)。ステップ195もしくはステップ197が実行されたら、 $R$ を送信部291より検証器3へ送信する(ステップ196)。

【0229】検証器3は、受信部282において証明器2から送信された $R$ を受信して、情報保持部289に記録する(ステップ133)。 $y'$ を第1の演算部283で計算して、その計算結果が $R$ と一致するかを、正当性検証部285で判定する(ステップ134)。一致すると判定された場合は証明器2が有効なチケットを持っていることを示すので、「有効」を意味する出力を出力部2812より出力する。一致しないと判定された場合は証明器2が有効なチケットを持っていることが示されなかったので、「無効」を意味する出力を出力部2812より出力する。

【0230】以上が第14の対話プロトコルである。第14のプロトコルでは、最初の簡単なプロトコルと同様の機能を提供している。

【0231】

〔表13〕

```

61
検証器
公開情報:  $y$ 
出力: '有効' もしくは '無効'
 $r := \text{rand}$ 
 $C := g^r$ 
send ( $C, y$ )
receive  $R$ 
if  $y^r = R$ 

    output '有効'
else
    output '無効'

Prover
if time <  $L$ 
     $R = C^a$ 
else
     $R = 1$ 

```

62

【0232】 [3. 3. 第15の対話プロトコル]  
 (使い捨て型の回数券型のチケット、図19、図32、  
 図33) 第15の対話プロトコルで利用するチケット補  
 助情報Lには、検証器3の公開情報 $\eta$ と、カウンタ $i$ 、  
 の上限値 $l$ が含まれていることを前提にする。第15の  
 対話プロトコルにおける検証器3の手順を図32に、証  
 明器2の手順を図19にそれぞれ従って説明する。

【0233】 検証器3は、認証情報生成部286によっ  
 て乱数 $r$ を生成して、 $C := g^r$ としてチャレンジ $C$ を  
 生成して、認証情報保持部287に記録する(ステップ  
 321)。認証情報保持部287に記録された $C$ と、公  
 開情報 $y$ をまとめて、送信部281より証明器2へ送信  
 する(ステップ322)。

【0234】 ステップ191の代わりに、証明器2は、  
 検証器3から送信された( $C, y$ )を受信部292で受  
 信して、情報保持部299に記録する。チケット探索部  
 122は受信した $y$ に対応するチケットをチケット保持  
 部121から探して、チケットを持っているかどうかを  
 判定する(ステップ192)。対応するチケットを持た  
 ない場合には、レスポンス $R$ に0を設定して、情報保持  
 部299に記録する(ステップ197)。対応するチケ  
 ットを持つ場合には、チケット $t$ 、証明器2の手順Pr  
 over $_2$ 、チケット付加情報 $L$ をセットする(ステッ  
 プ193)。Prover $_2$ のセットとして、 $L$ より  
 ( $\eta, i$ )を取り出しておく。

【0235】 ステップ193が実行されたら、ステップ  
 194を実行する。本プロトコルにおけるステップ19  
 4の詳細な手順を図33に従って説明する。認証情報生  
 成部296チャレンジで乱数 $s$ を生成して、 $x := g^s$   
 としてチャレンジ $x$ を生成して、第2の認証情報保持部

298に記録する(ステップ331)。送信部291か  
 ら検証器2に $x$ を送信する(ステップ332)。

【0236】 検証器3は、 $x$ を受信部282で受信し  
 て、情報保持部289に記録する(ステップ323)。  
 受信した $x$ が0の場合は、チケットが無くて $R$ が0とし  
 て送られたことを示すので、「無効」意味する出力を出  
 力部2812より出力して、対話プロトコルを終了する  
 (ステップ324)。第2の演算部284においてレス  
 ポンス $\rho$ を、

【0237】

【数35】

$$\rho := x^f$$

として計算する(ステップ325)。計算した $\rho$ を送信  
 部281より証明器2へ送信する(ステップ326)。

【0238】 証明器2は、 $\rho$ を受信部292で受信し  
 て、情報保持部299に記録する(ステップ333)。  
 第2の演算部294で $\eta'$ を計算して、受信した $\rho$ と一  
 致するか判定する(ステップ334)。判定の結果とし  
 て一致する場合には、内部状態保持部124の第2の内  
 部状態保持部に確保されているカウンタ $i$ の値をイン  
 クリメントする(ステップ335)。ステップ335が  
 実行されたら、 $i$ の値を $l$ より得られた上限値 $l$ と比  
 較する(ステップ336)。ステップ337の比較の結果  
 として、 $i$ の値が $l$ 以下の場合には、第1の演算部2  
 93で $R := C'$ を計算して、情報保持部299に記録  
 する(ステップ337)。ステップ337の比較の結果  
 として、 $i$ の値が $l$ より大きい場合は、内部状態保持  
 部124の第2の内部状態保持部から $i$ を解放して、  
 チケット保持部121からチケットを削除して(ステッ  
 プ338)。ステップ334で一致しなかった場合と合

63

わせてRに1を設定して、情報保持部299に記録する(ステップ339)。ここまでが第15の対話プロトコルにおけるステップ194の詳細な手順である。

【0239】ステップ194が実行されたら、ステップ193でセットされた $t$ 、 $Prover$ 、 $L$ を解除する(ステップ195)。ステップ195もしくはステップ197が実行されたら、送信部291から検証器3へRを送信する(ステップ196)。

【0240】検証器3は、受信部282において証明器2から送信されたRを受信して、情報保持部289に記録する(ステップ327)。y'を第1の演算部283で計算して、その計算結果がRと一致するかを、正当性

#### 検証器

```

r := rand
C := gr
send (C, y)
receive x
ρ := xε
receive R
if yr = R
    output '有効'
else
    output '無効'

```

#### Prover

```

s = rand
χ := gs
send χ
receive ρ
if ηs = ρ
    i := i + 1
    R = Cs
else
    R = 1

```

【0243】【4. 第3の実施例】

(チケットの初期化、図5～図12) この第3の実施例において、チケット作成・発行装置1とチケット証明器2は、チケットの多重初期化を回避するために、チケット

【0244】チケット作成・発行装置1においては、チケットカウント手段は証明器固有情報保持手段(データベース)7に含ませる構成にしても構わない。また、チケット証明器2においては、チケットカウント手段は内容の書き換えが行なえないような防衛機構を設けてあればより適切である。

【0245】なお、チケット作成・発行装置1によるチケット作成・発行の全体の動作については第4の実施例を参照して後に詳述する。

64

検証部285で判定する(ステップ328)。一致すると判定された場合は証明器2が有効なチケットを持っていることを示すので、「有効」を意味する出力を出力部2812より出力する。一致しないと判定された場合は証明器2が有効なチケットを持っていることが示されなかったので、「無効」意味する出力を出力部2812より出力する。

【0241】以上が第15の対話プロトコルである。本プロトコルは、第1の実施例の第3の対話プロトコルと同様の機能を提供する。

【0242】

【表14】

【0246】チケット発行の手順を図5を参照して説明する。図5において、チケット発行時、ステップ55において、そのチケットが証明器2内部の状態を初期化すると判定されれば、チケット作成・発行装置1のチケットカウント手段からカウンタ値を取り出してチケットと共に送る。初期化が不要な場合は $i = 0$ を送る。チケットカウンタ値は最初に1に設定されている。ステップ56においては次回のチケット発行要求に備えるためにカウンタ値を1増加する。チケットは公開情報だが完全性を保つ必要はある。したがって、センターが署名手段を持ち、証明器識別子とカウンタ値とチケット識別子と初期化手順と証明手順とチケット付加情報とに署名を施すのは好適である。

【0247】図6は、発行されたチケットの証明器2へ

の登録を行なう手順を表している。図 6 において、ステップ 6 1 でチケット保持部に余裕があることを確認し、ステップ 6 2 でチケットへの署名の検証を行なう。ステップ 6 3 で証明器識別子が正しいことを確認し、ステップ 6 4 で  $i$  の値により初期化が必要かどうかを判定する。初期化が必要と判定されるとステップ 6 5 で  $i$  の値が初期化の必要なチケットとしてはじめて現れたかどうかを判定する。

【0248】この判定の手順は図 7 で説明される。はじめてのチケット登録と判定されればステップ 6 6 で初期化が実行される。初期化の実行例は図 8 および図 9 で例を挙げて説明する。初期化が不要な場合はチケット保持手段に入力されたチケットを登録する。

【0249】図 7 は、内部状態多重初期化回避の判定を行なう手順を表している。ここでは、証明器 2 の内部状態保持手段には通し番号のリストを保持する手段を設ける構成として説明する。

【0250】チケットカウント手段に保持された  $i$  は、今までに初期化が行なわれたチケットの通し番号  $i$  のうち最大のものであり、内部状態保持手段に保持されたリストは  $i$  より小さい通し番号のうち未だ初期化されていないものからなる。

【0251】入力された通し番号  $i$  に対して、まずステップ 7 1 でチケットカウント手段に保持された  $i$  との比較を行なう。 $i > i$  であれば通し番号  $i$  に対応する初期化はまだ行なわれていないので、ステップ 7 2 へ進み、そうでないならばステップ 7 4 へ進む。ステップ 7 2 では、 $i$  より大きく  $i$  より小さい初期化が未だ行なわれていない通し番号をリストに加える。もしも、リストに加えることができなければリストのオーバーフローなので例外処理を行なう。ついでステップ 7 3 では、 $i$  の値を  $i$  で置き換えて、OK を出力する。

【0252】ステップ 7 4 では、 $i$  が内部状態保持手段に保持されたリストに存在するかどうかを判定する。リストにあれば、ステップ 7 5 で  $i$  をリストから削除し、OK を出力する。リストになければ、NG を出力する。

【0253】図 8 と図 9 はチケットに対する内部状態の初期化の手順を表している。図 8 および図 9 において、まず、ステップ 8 1、9 1 で初期化の領域確保が可能かどうか判断し、可能であれば、ステップ 8 2 または 9 2 において内部状態  $i$  をゼロまたは  $L$  に初期化する。

【0254】また、証明器 2 からのチケットの削除は図 10 に示すようにパスワードによる認証で行うことができる。また内部状態の開放も図 11 に示すように同様にパスワードによる認証で行うことができる。

【0255】〔第 4 の実施例〕

(チケット作成・発行装置 1 のチケット作成・発行、図 2、図 3、図 4、図 5) 第 4 の実施例としてチケット作成・発行装置 1 を説明する。図 4 はチケット作成の手順を示している。

【0256】チケット作成手段 4 は、チケットの仕様を指示したチケット作成依頼を受け取る。ここでチケットの仕様とは、チケットの検証手順と証明手順と初期化手順とチケット付加情報のデータの型とチケット発行依頼者の資格情報とからなる。

【0257】手順の指定には手順に対する識別子を用意して、その識別子で指示しても良いし、手順自体を与えるようにしても良い。以下では、仕様の識別子によって指定する方法を述べる。また、チケットが内部状態を持ち、特権を持つ検証者がその内部状態を変更できる場合は、検証手順と証明手順を決定するためには、検証者の特権に対応する証明証も与える必要がある。

【0258】図 4 において、チケット作成手段は、チケット作成依頼を受けるとステップ 4 1 において仕様を検索する。ついで、ステップ 4 2 においてチケットの特徴情報を生成する。ここでは、RSA 公開鍵暗号系の公開鍵ペアを特徴情報とするものとする。チケットの特徴情報はチケットの作成依頼に応じて作成しても良いし、予め作成して用意しておいても良い。ステップ 4 3 において特徴情報と仕様の識別子とチケット付加情報のデータの型とチケット発行依頼者の資格情報(と必要ならば特権を持つ検証者の証明証)の組をチケット原型データベース 6 に記憶する。ステップ 4 4 においてチケット識別子  $n$  とチケット公開情報  $E$  とチケット仕様  $S$  に対応するチケット検証手順  $Verifier$  に対して署名を行ない、それをチケット作成依頼者に与える。

【0259】図 5 はチケット発行の手順を表している。図 5 において、チケット発行依頼者は、チケット識別子と証明器識別子とチケット仕様識別子とチケット付加情報により、チケットを指定して発行の依頼を行なう。この際、チケット発行手段 5 はチケット発行依頼者の資格をチケット原型データベースに記憶された資格情報にてらして確かめる。チケット発行手段 5 は、まず、ステップ 5 1 において証明器識別子に対応する固有情報を検索する。ステップ 5 2 においてチケット識別子に対応するチケットの原型を検索する。ステップ 5 3 において仕様識別子に対応する仕様を検索する。ステップ 5 4 において与えられたチケット付加情報の型が正しいかどうかを判定する。ステップ 5 5 においてチケットが初期化を伴うかどうかを判定する。チケットが初期化を伴うならば、ステップ 5 6 において、証明器固有情報データベース 7 に記憶された  $i$  を  $i$  にセットし、ステップ 5 7 において  $i$  をインクリメントする。ステップ 5 5 においてチケットが初期化を伴わないと判定されれば、ステップ 5 8 において  $i$  を 0 にセットする。ステップ 5 9 において、今までの実施例で述べたように  $D$ 、 $d$ 、 $L$  よりチケット  $t$  を生成する。ステップ 5 10 において証明器識別子  $U$  と初期化を伴うチケットの通し番号  $i$  とチケットの初期化手順  $Init$  とチケットの証明手順  $Prover$  とチケット付加情報  $L$  とチケット  $t$  との組にチ

ケット発行手段の署名をつけて発行を行なう。

【0260】

【発明の効果】これまで述べたように、電子チケットを実現するためには、以下の機能を満たす必要がある。第1点は、正当な権利を持たないものが、不当にチケットを利用することを防止する機能である。第2点は、利用者が自分の保持するチケットの正当性を確認できる機能である。第3点は、当事者間で争いが生じたときに備えて、チケットに与えられた権利内容を第三者に証明できる機能である。さらに状況に応じては、第4点として利用者の匿名性が保証される必要がある。

【0261】本発明によれば、複製が非常に困難な証明器とそれに対応するチケットがない限り不正利用が不可能であり、第1の機能を満たす。また、誰が知っている問題のない公開された情報だけで、利用者の持つチケットの内容を証明できるので、第2および第3の機能を満たす。さらに、チケットの検証時に利用者に依存する情報がまったく通信されないで、利用者の匿名性が維持されて、第4の機能を満たす。このように、本発明によれば、以上の4点すべての機能を満たしたチケットの作成・発行・利用システムが実現される。加えて、チケット発行時および検証時の情報の通信をすべて開示できるので、利用者がその内容を確認することで、利用者の権利を侵害する通信が行われていないことを証明する効果も併せ持つ。

【図面の簡単な説明】

【図1】 この発明の原理的な構成例を示すブロック図である。

【図2】 チケット作成・発行装置の構成を示すブロック図である。

【図3】 チケット作成・発行装置の他の構成を示すブロック図である。

【図4】 チケット作成・発行装置の動作を説明するフローチャートである。

【図5】 チケット作成・発行装置の動作を説明するフローチャートである。

【図6】 証明器へのチケット登録の動作を説明するフローチャートである。

【図7】 多重初期化の判定ルーチンを説明するフローチャートである。

【図8】 証明器の内部状態初期化の一例を説明するフローチャートである。

【図9】 証明器の内部状態初期化の一例を説明するフローチャートである。

【図10】 証明器からチケットを削除する手順を説明するフローチャートである。

【図11】 証明器から内部状態を開放する手順を説明するフローチャートである。

【図12】 チケット検証器およびチケット証明器の構成を示すブロック図である。

【図13】 チケット検証の手順を説明するフローチャートである。

【図14】 チケット検証の手順を説明するフローチャートである。

【図15】 チケット検証の手順を説明するフローチャートである。

【図16】 チケット検証の手順を説明するフローチャートである。

【図17】 チケット検証の手順を説明するフローチャートである。

【図18】 チケット検証の手順を説明するフローチャートである。

【図19】 チケット証明の手順を説明するフローチャートである。

【図20】 チケット証明手順の一部を説明するフローチャートである。

【図21】 チケット証明手順の一部を説明するフローチャートである。

【図22】 チケット証明手順の一部を説明するフローチャートである。

【図23】 チケット証明手順の一部を説明するフローチャートである。

【図24】 チケット証明手順の一部を説明するフローチャートである。

【図25】 チケット証明手順の一部を説明するフローチャートである。

【図26】 チケット証明手順の一部を説明するフローチャートである。

【図27】 チケット証明手順の一部を説明するフローチャートである。

【図28】 検証手順実行手段の構成を示すブロック図である。

【図29】 証明手順実行手段の構成を示すブロック図である。

【図30】 チケット検証器の構成を示すブロック図である。

【図31】 チケット証明手順を説明するフローチャートである。

【図32】 チケット検証の手順を説明するフローチャートである。

【図33】 チケット証明手順を説明するフローチャートである。

【符号の説明】

- 1 チケット作成・発行装置
- 2 チケット証明装置
- 3 チケット検証装置
- 4 チケット作成手段
- 5 チケット発行手段
- 6 チケット原型データベース
- 7 証明器固有情報データベース

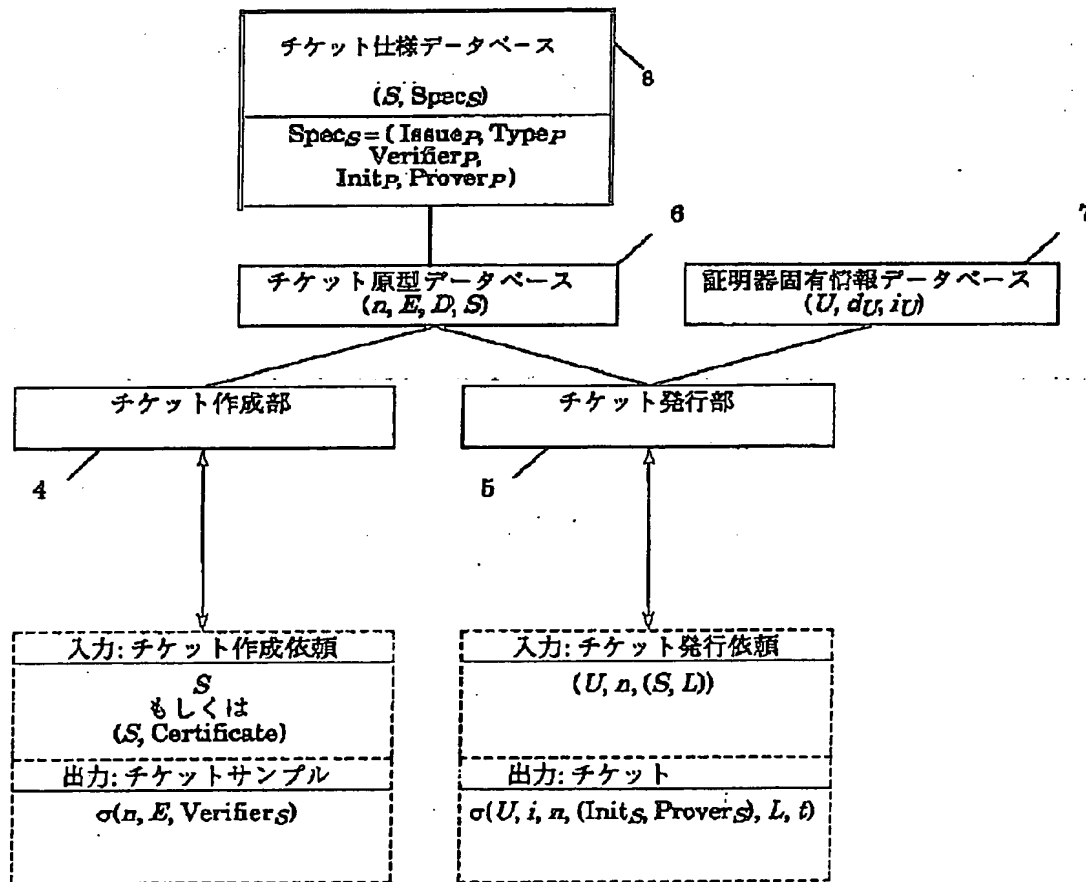
69

70

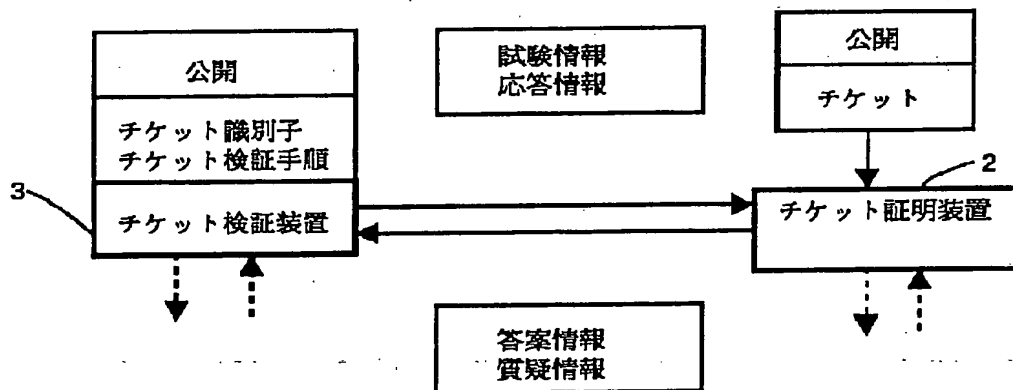
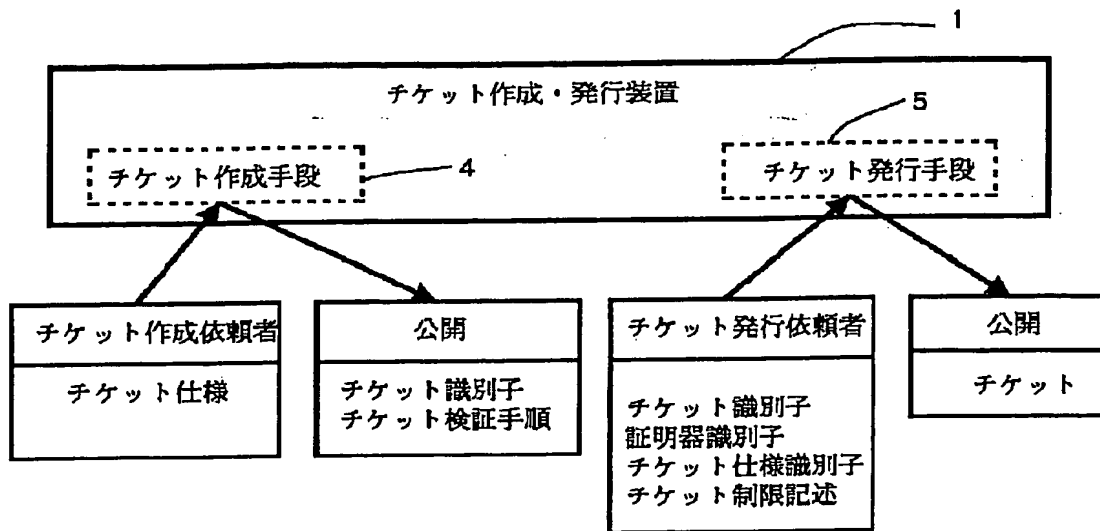
1 1 1 検証手順実行部  
 1 1 2 通信部  
 1 2 1 チケット保持部  
 1 2 2 チケット検索部  
 1 2 3 固有情報保持部  
 1 2 4 内部状態保持部  
 1 2 5 証明手順実行部  
 1 2 6 通信部  
 2 8 1 検証手順実行部 1 1 1 の送信部  
 2 8 2 検証手順実行部 1 1 1 の受信部  
 2 8 3 検証手順実行部 1 1 1 の第 1 の演算部  
 2 8 4 検証手順実行部 1 1 1 の第 2 の演算部  
 2 8 5 検証手順実行部 1 1 1 の正当性検証部  
 2 8 6 検証手順実行部 1 1 1 の認証情報生成部  
 2 8 7 検証手順実行部 1 1 1 の認証情報保持部  
 2 8 8 検証手順実行部 1 1 1 のチケット識別子保持部  
 2 8 9 検証手順実行部 1 1 1 の情報保持部  
 2 8 1 0 検証手順実行部 1 1 1 の出力情報保持部

2 8 1 1 検証手順実行部 1 1 1 の入力情報保持部  
 2 8 1 2 検証手順実行部 1 1 1 の出力部  
 2 8 1 3 検証手順実行部 1 1 1 の入力部  
 2 8 1 4 検証手順実行部 1 1 1 の利用証拠情報保持部  
 2 8 1 4  
 2 9 1 証明手順実行部 1 2 5 の送信部  
 2 9 2 証明手順実行部 1 2 5 の受信部  
 2 9 3 証明手順実行部 1 2 5 の第 1 の演算部  
 2 9 4 証明手順実行部 1 2 5 の第 2 の演算部  
 2 9 5 証明手順実行部 1 2 5 の正当性検証部  
 2 9 6 証明手順実行部 1 2 5 の認証情報生成部  
 2 9 7 証明手順実行部 1 2 5 の認証情報保持部  
 2 9 8 証明手順実行部 1 2 5 の第 2 の認証情報保持部  
 2 9 9 証明手順実行部 1 2 5 の情報保持部  
 2 9 1 0 証明手順実行部 1 2 5 の出力情報保持部  
 2 9 1 1 証明手順実行部 1 2 5 の入力情報保持部  
 2 9 1 2 証明手順実行部 1 2 5 の制御部

〔図 3〕

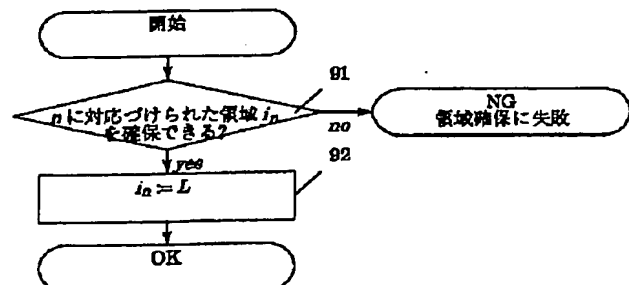
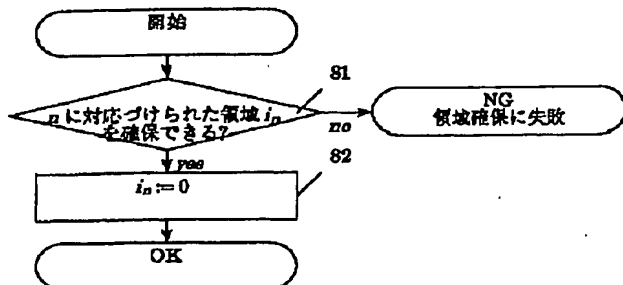


【図 1】

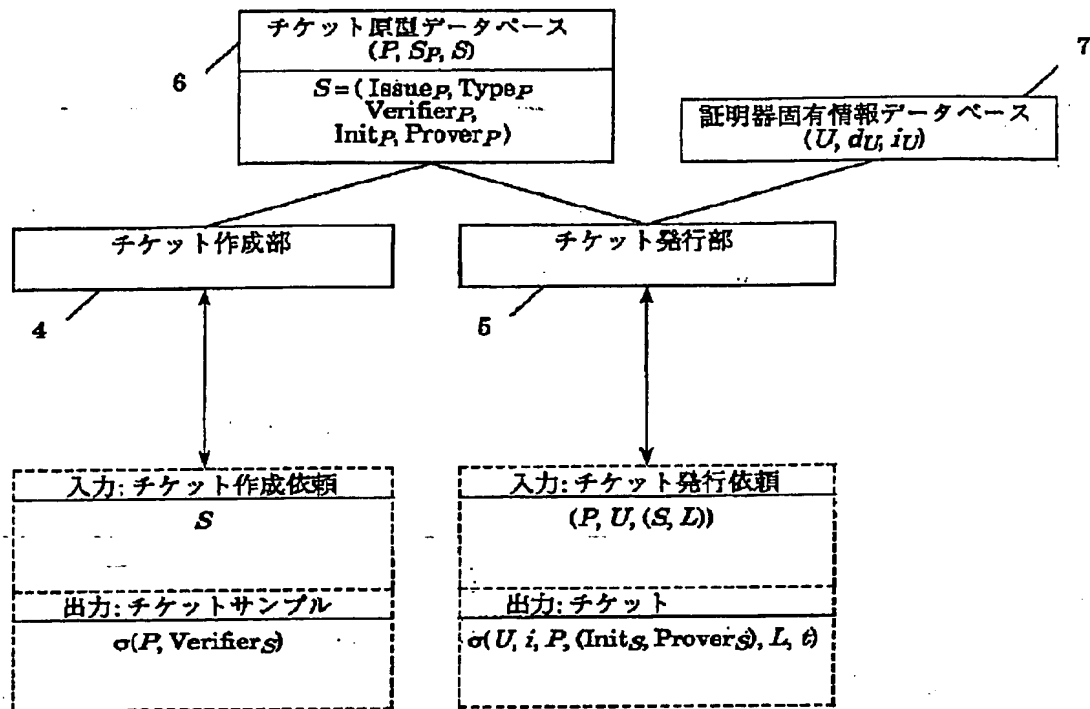


【図 8】

【図 9】

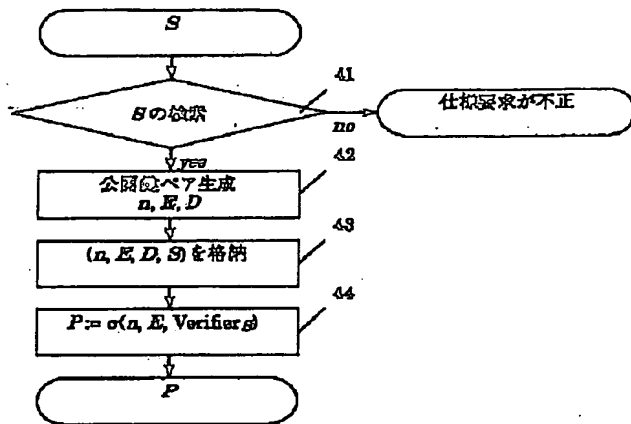


【図 2】

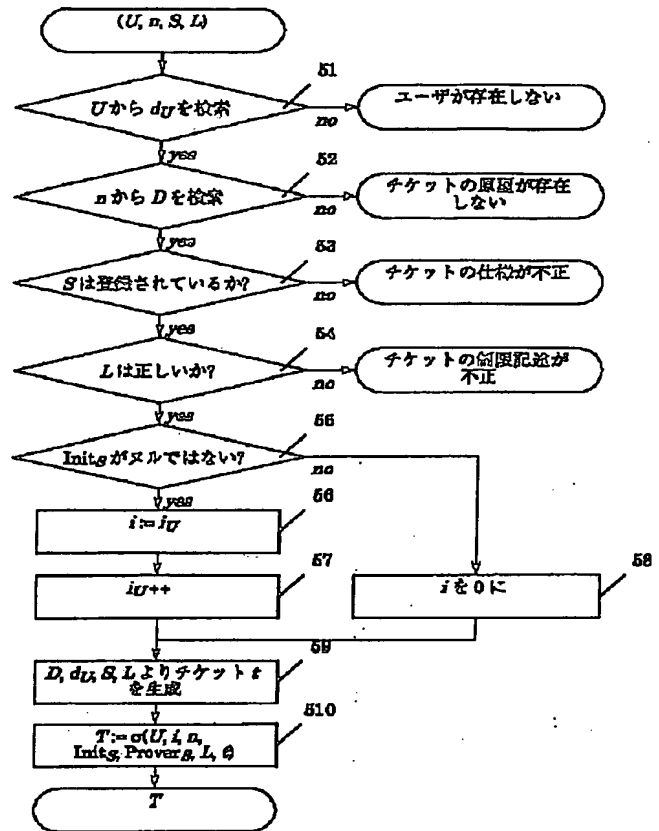




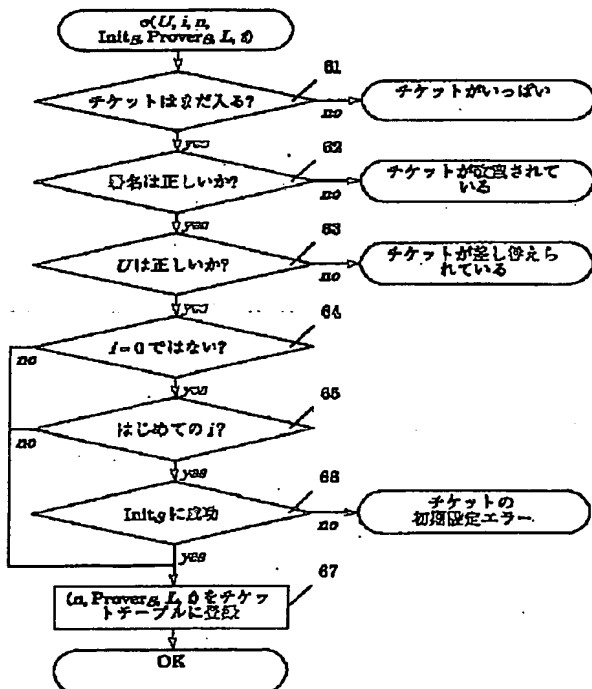
【図 4】



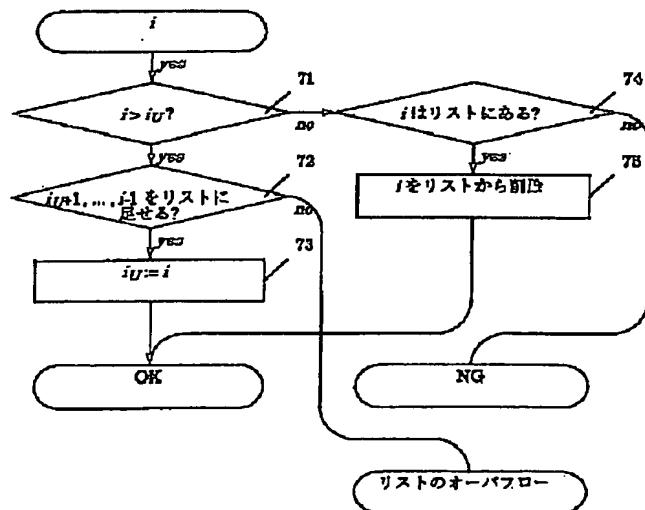
【図 5】



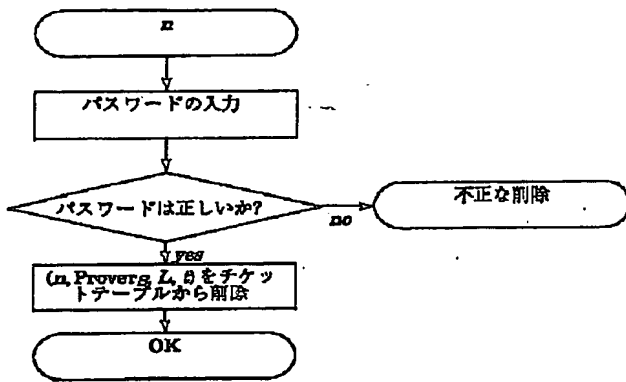
【図 6】



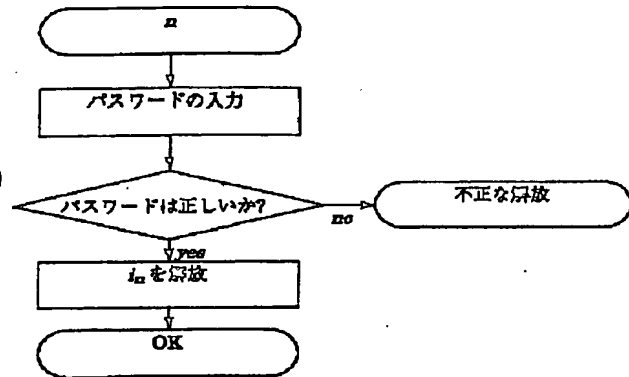
【図 7】



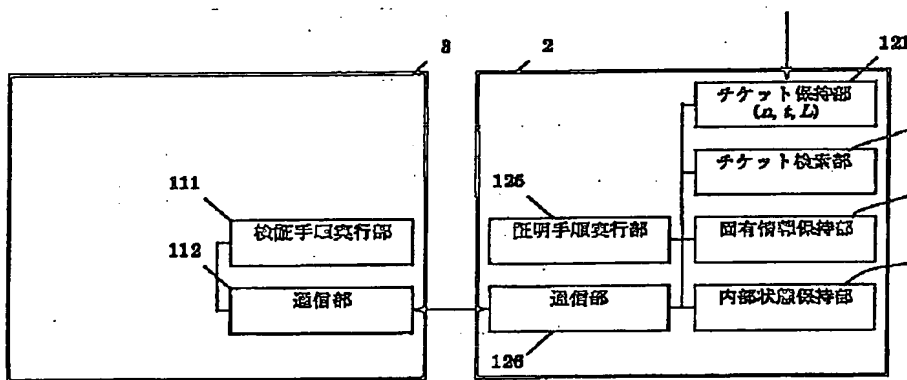
【図10】



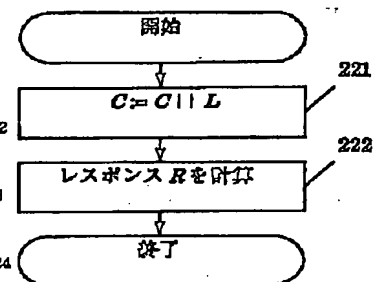
【図11】



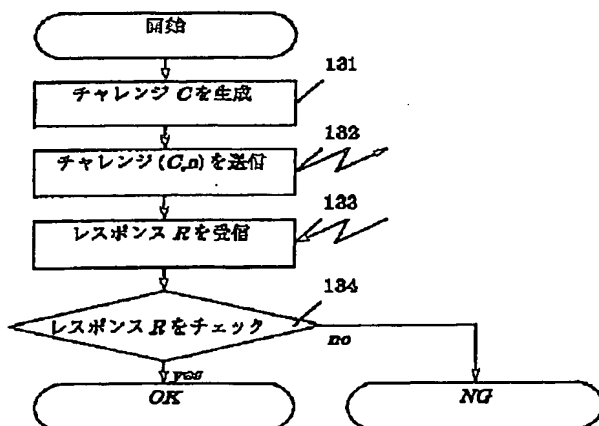
【図12】



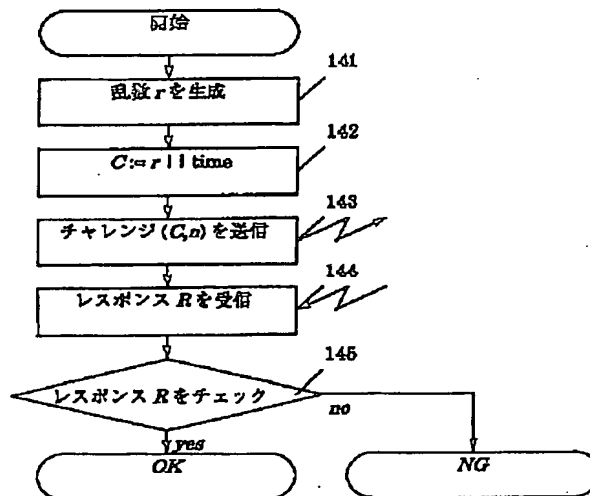
【図22】



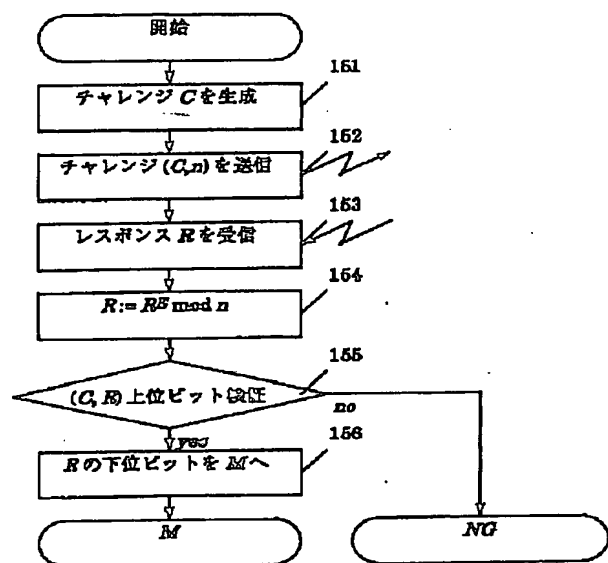
【図13】



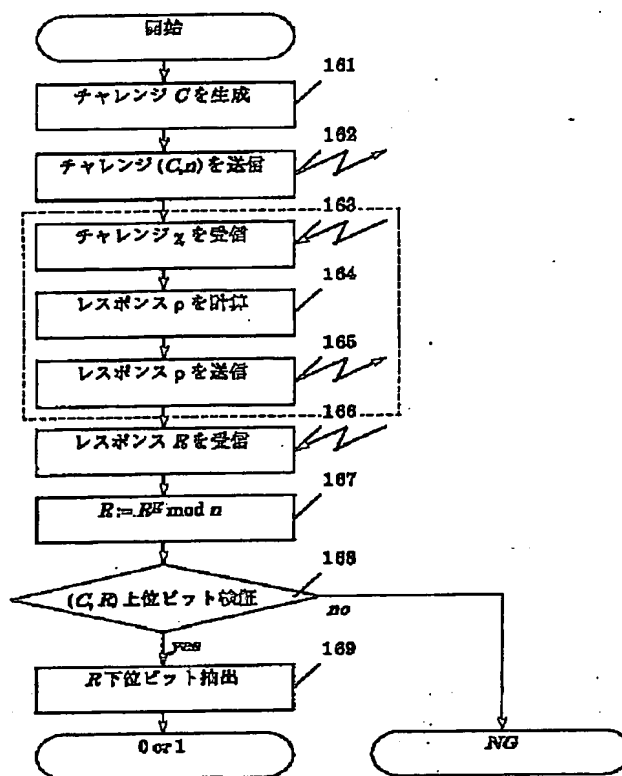
【図14】



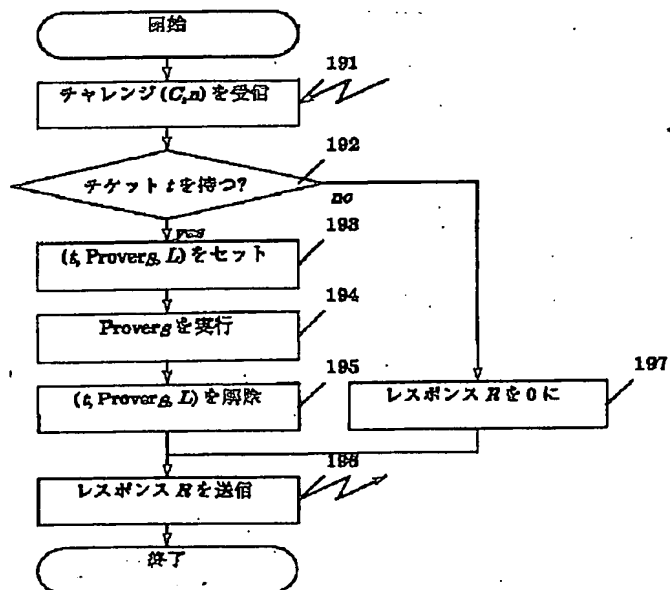
【図 15】



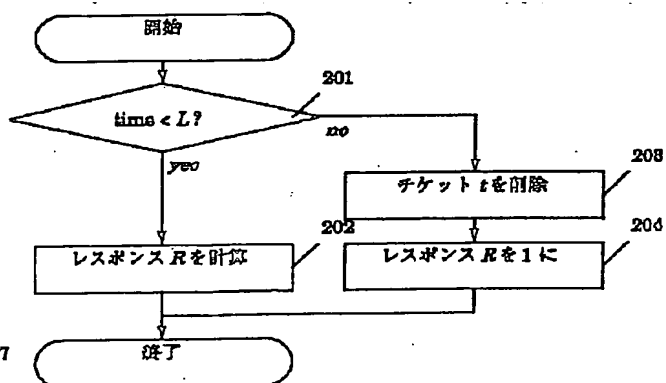
【図 16】



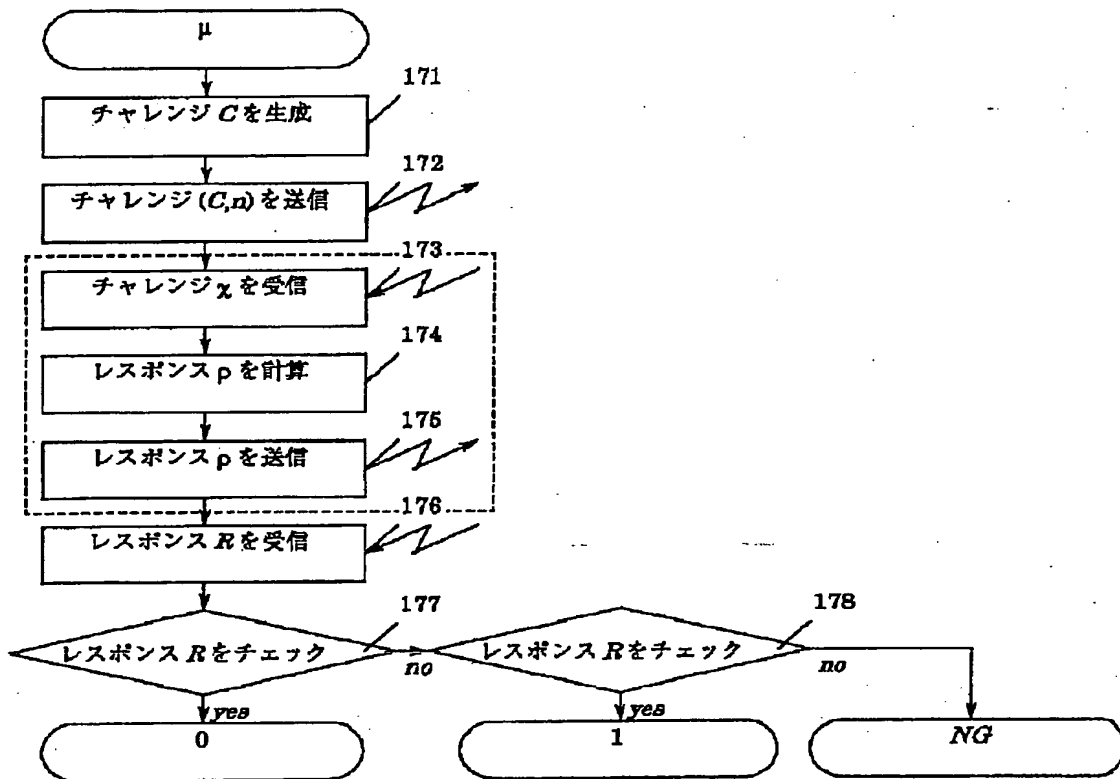
【図 19】



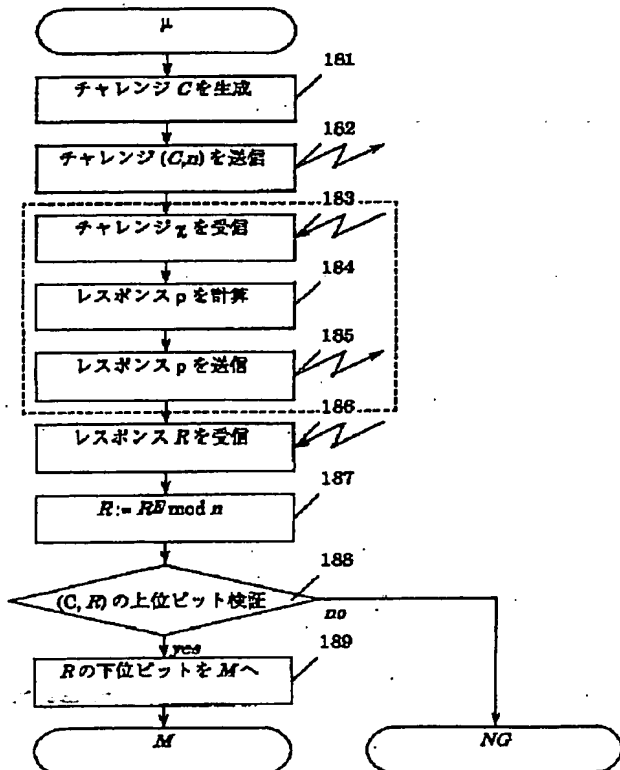
【図 20】



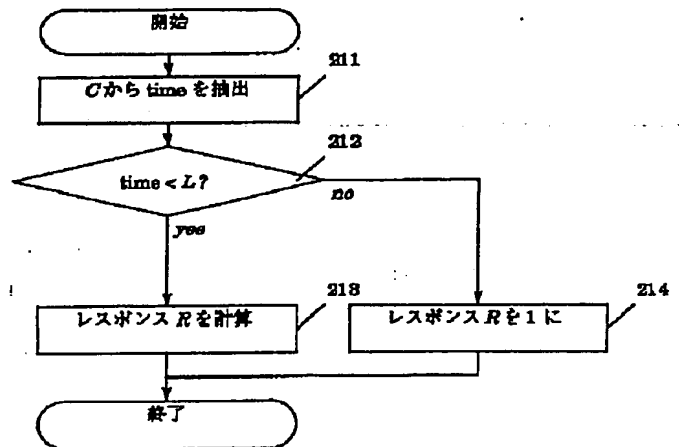
【図 17】



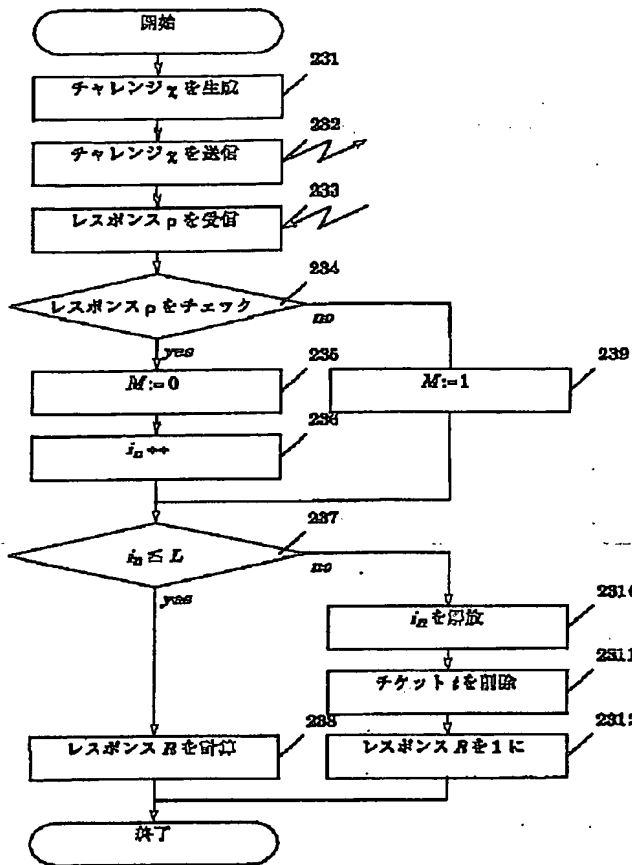
【図 18】



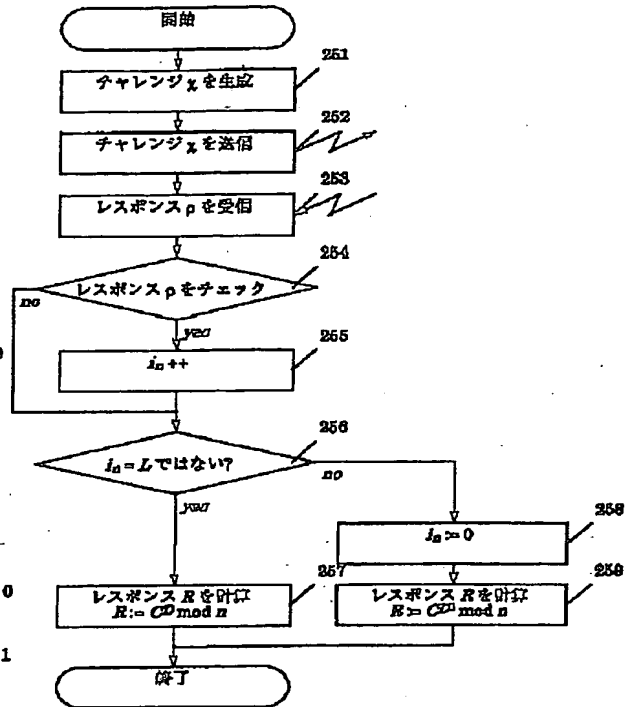
【図 21】



【図 2 3】

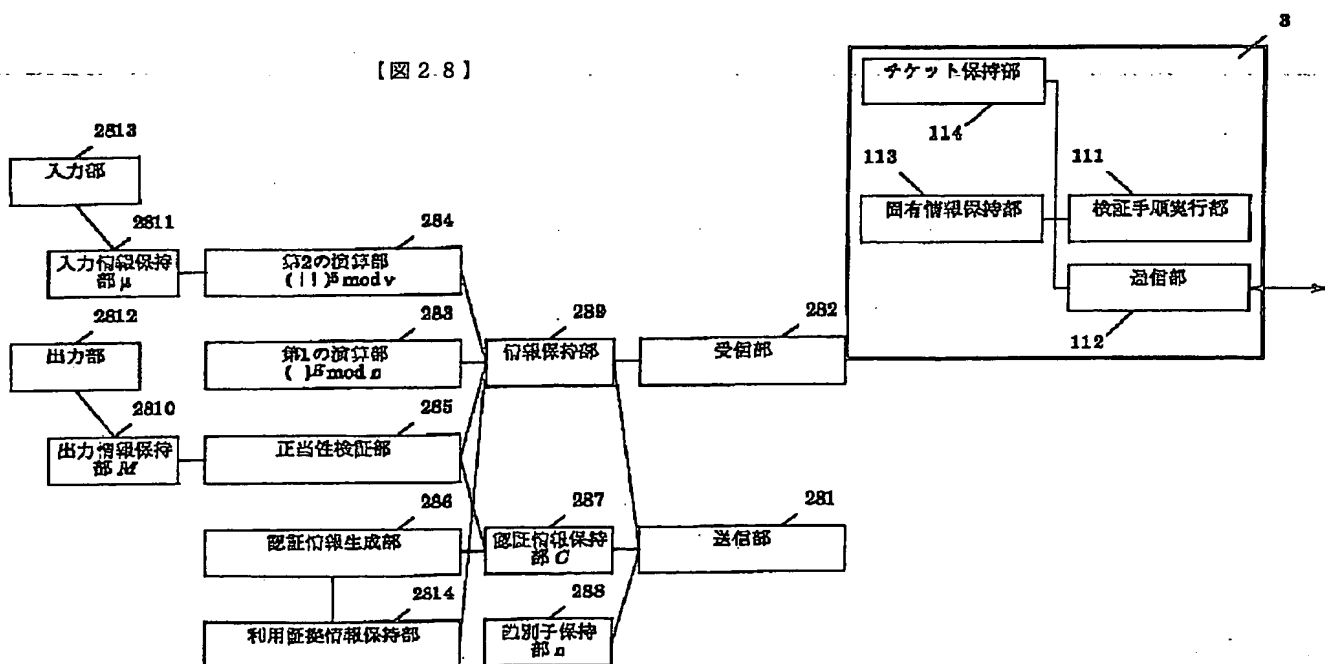


【図 2 5】

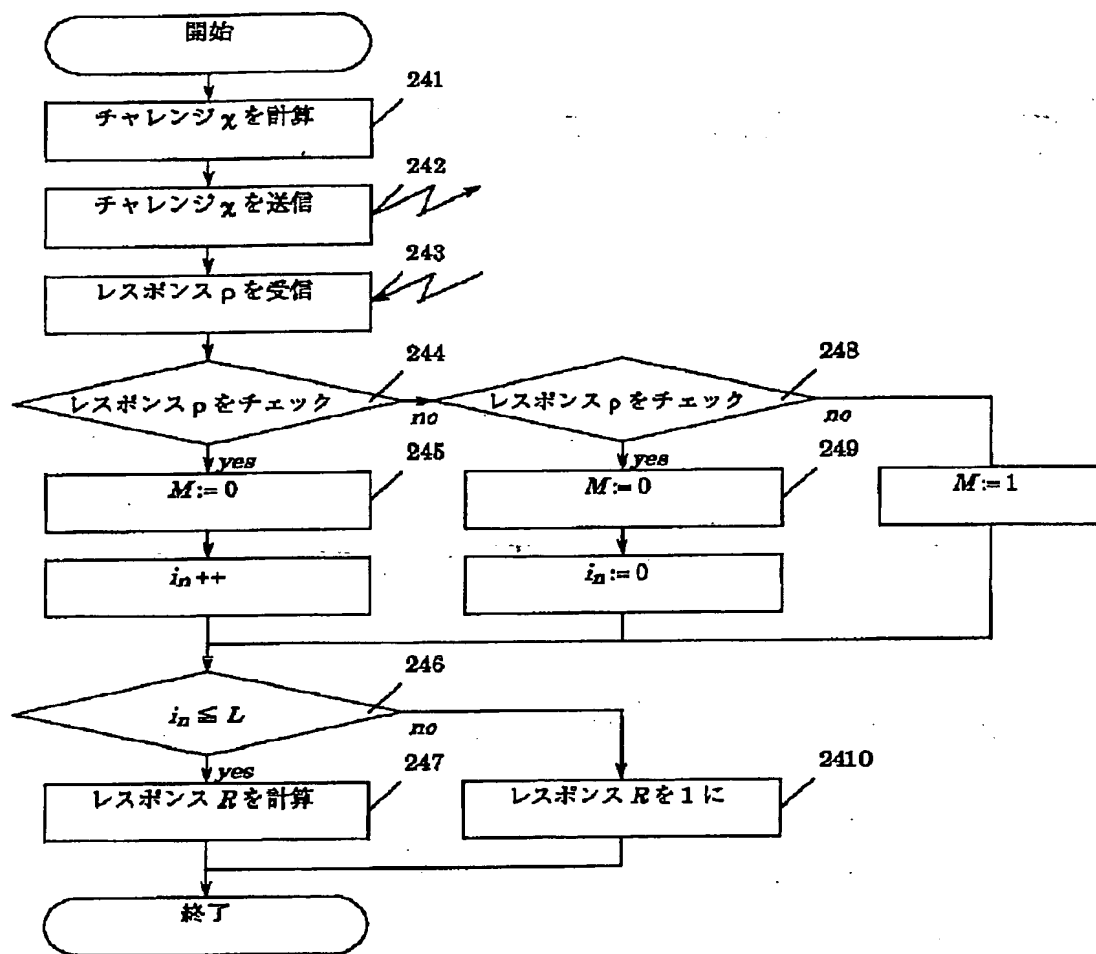


【図 3 0】

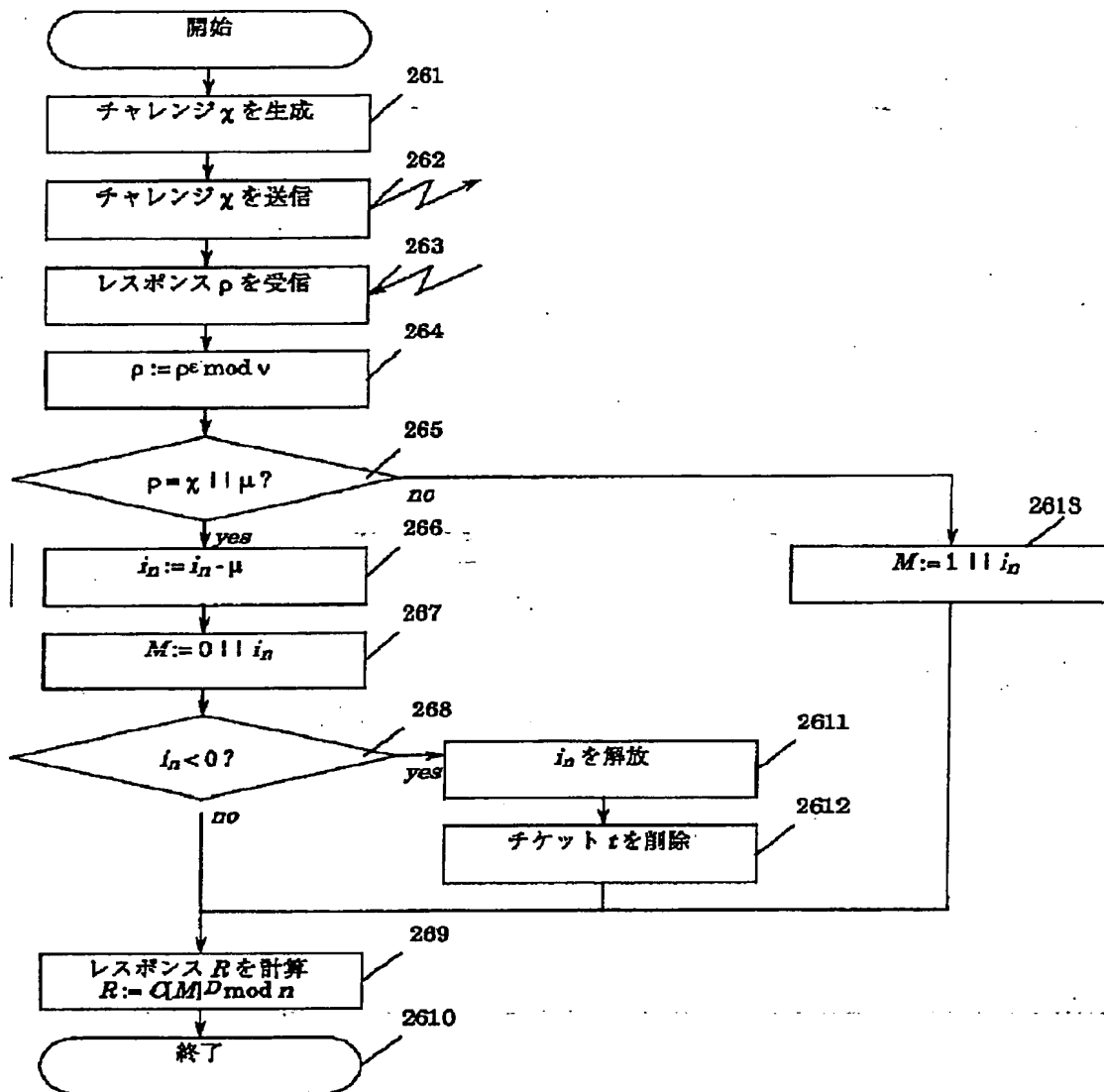
【図 2 8】



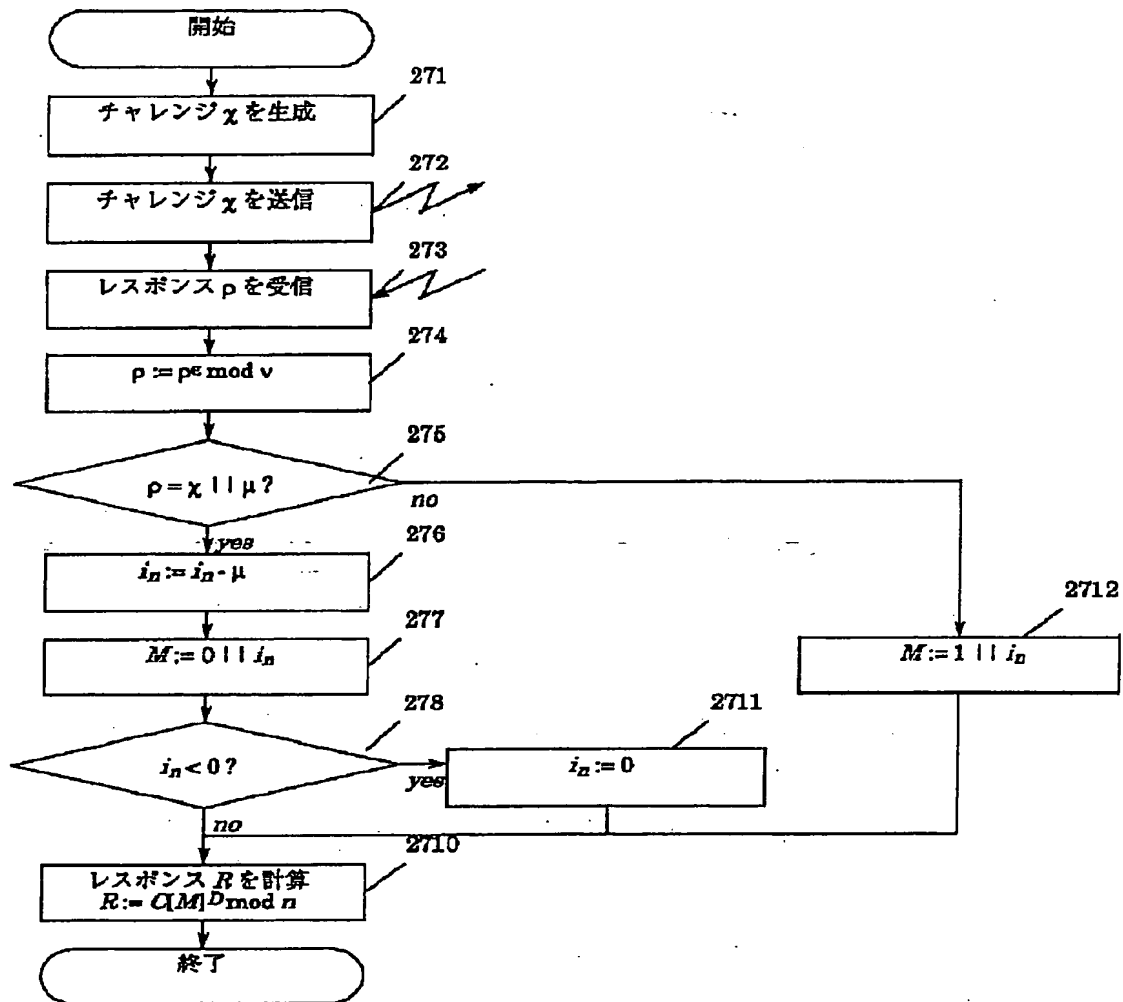
【図 2 4】



【図 26】

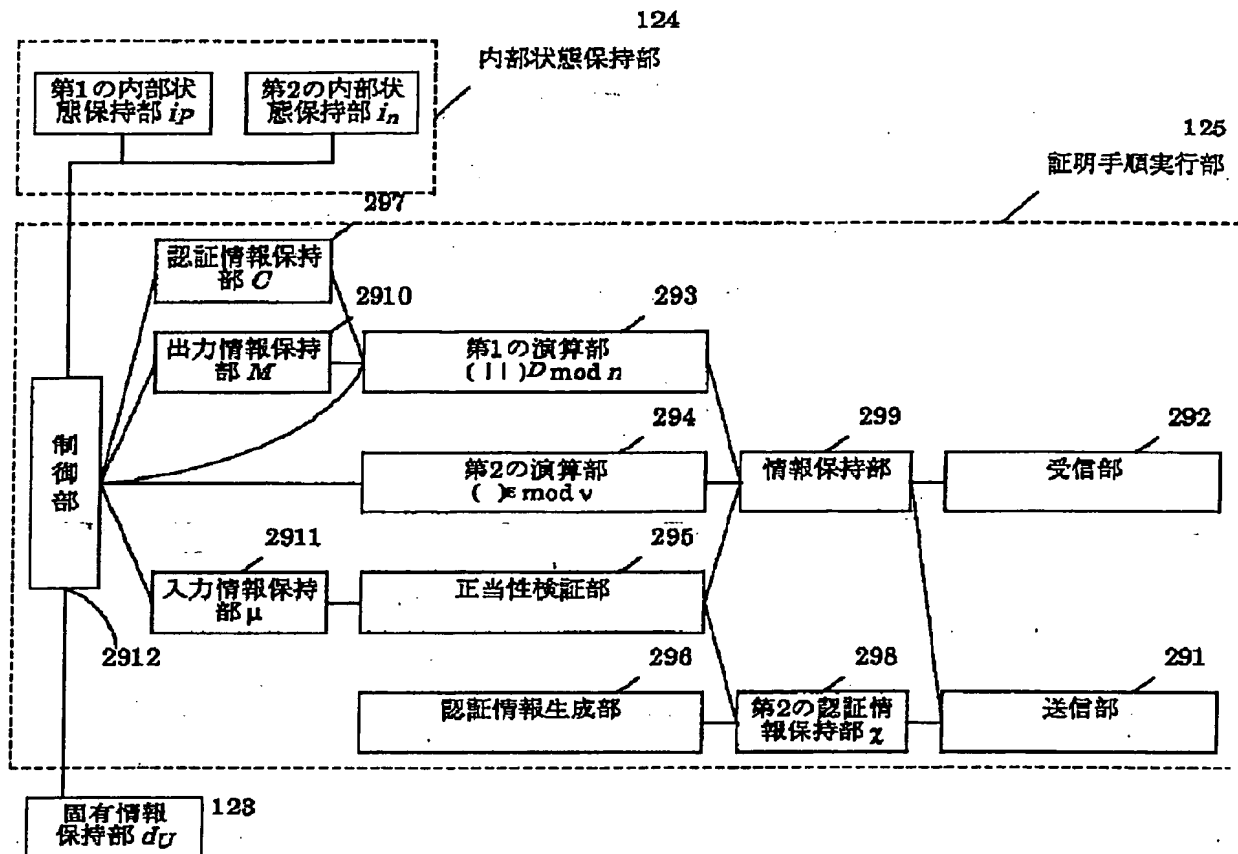


【図 27】

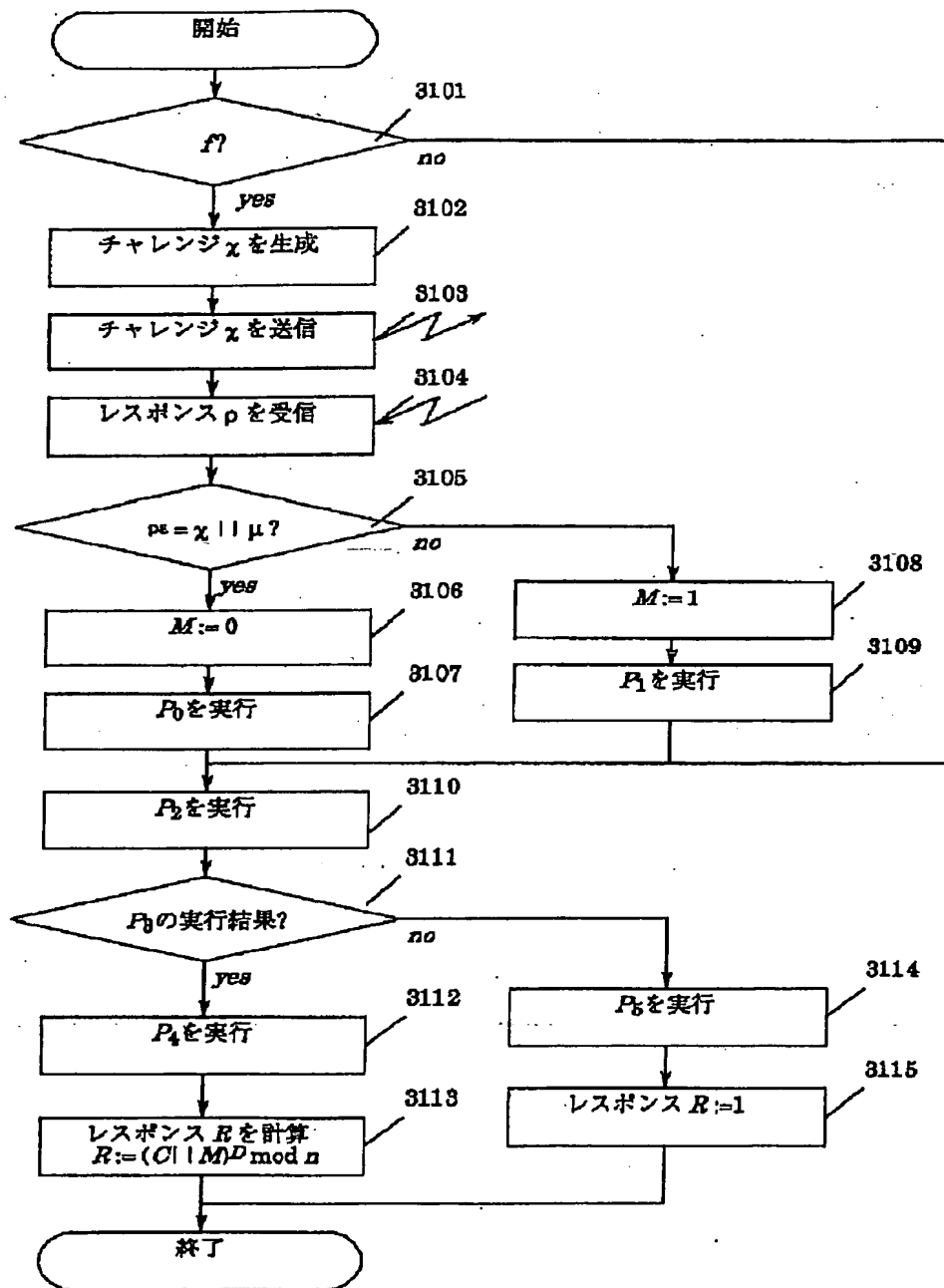




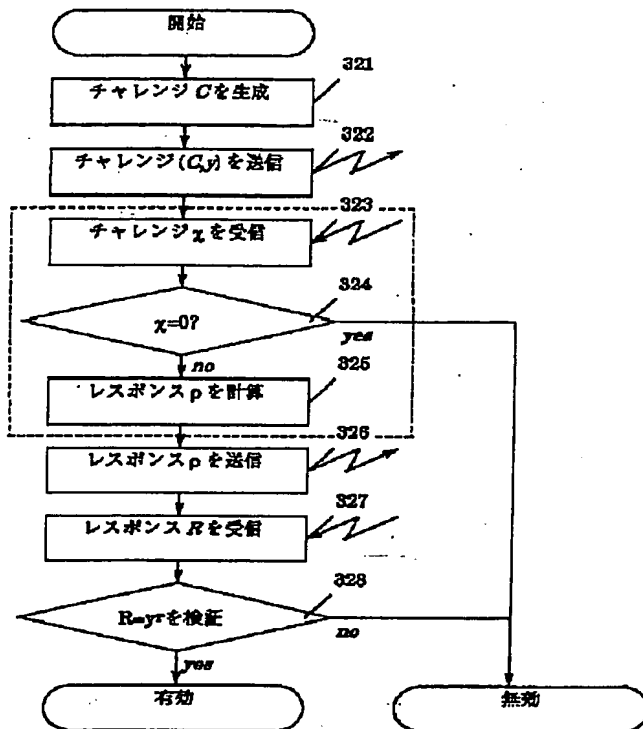
【図 29】



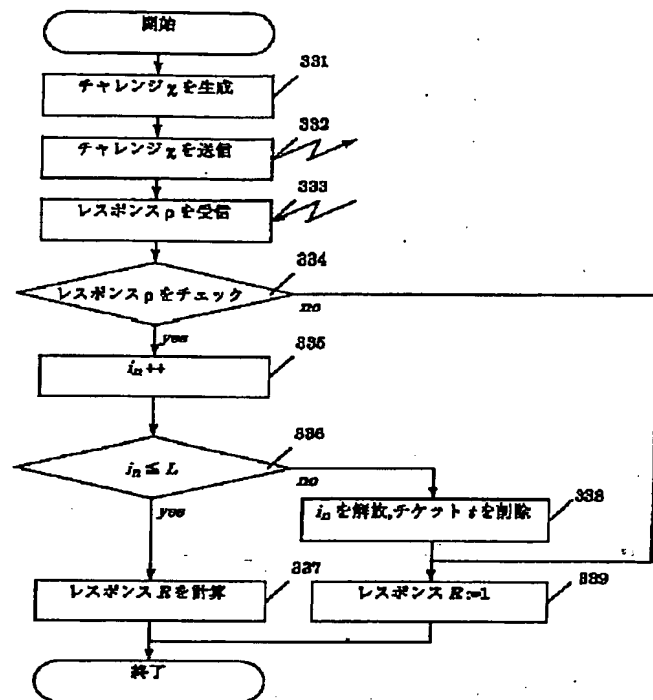
【図 3 1】



【図 3 2】



【図 3 3】



フロントページの続き

(51) Int. Cl.  
H04L 9/32

識別記号

庁内整理番号

F I

H04L 9/00

675

C

技術表示箇所